TI/TÜV Rheinland Functional Safety Seminar China

Texas Instruments Inc.

Nov/2014

Agenda

- Overview of Hercules™ MCU and SafeTI™ Design package
- Hercules™ MCU Functional Safety How-To Workshop
  - Safety Functions, Safety Goals, Safe State, SIL, Failure rate
  - Safety Critical Elements identification and Diagnostic Requirements
  - Safety Manual and Diagnostics Selection
  - Mission Profile and Failure Rate Estimation
  - SafeTI™ Diagnostic Library
  - SafeTI™ Diagnostic Library Compliance Support Package (CSP) certification support
  - Fault Injection with HITEX kit
- Summary

Agenda

- Overview of Hercules™ MCU and SafeTI™ Design package
- Hercules™ MCU Functional Safety How-To Workshop
  - Safety Functions, Safety Goals, Safe State, SIL, Failure rate
  - Safety Critical Elements identification and Diagnostic Requirements
  - Safety Manual and Diagnostics Selection
  - Mission Profile and Failure Rate Estimation
  - SafeTI™ Diagnostic Library
  - SafeTI™ Diagnostic Library Compliance Support Package (CSP) certification support
  - Fault Injection with HITEX kit
- Summary

Functional Safety: Important for Many Industries

Automotive and Transportation



HEV/EV Cars



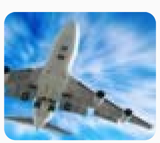
Radar / Collision Avoidance (ADAS)



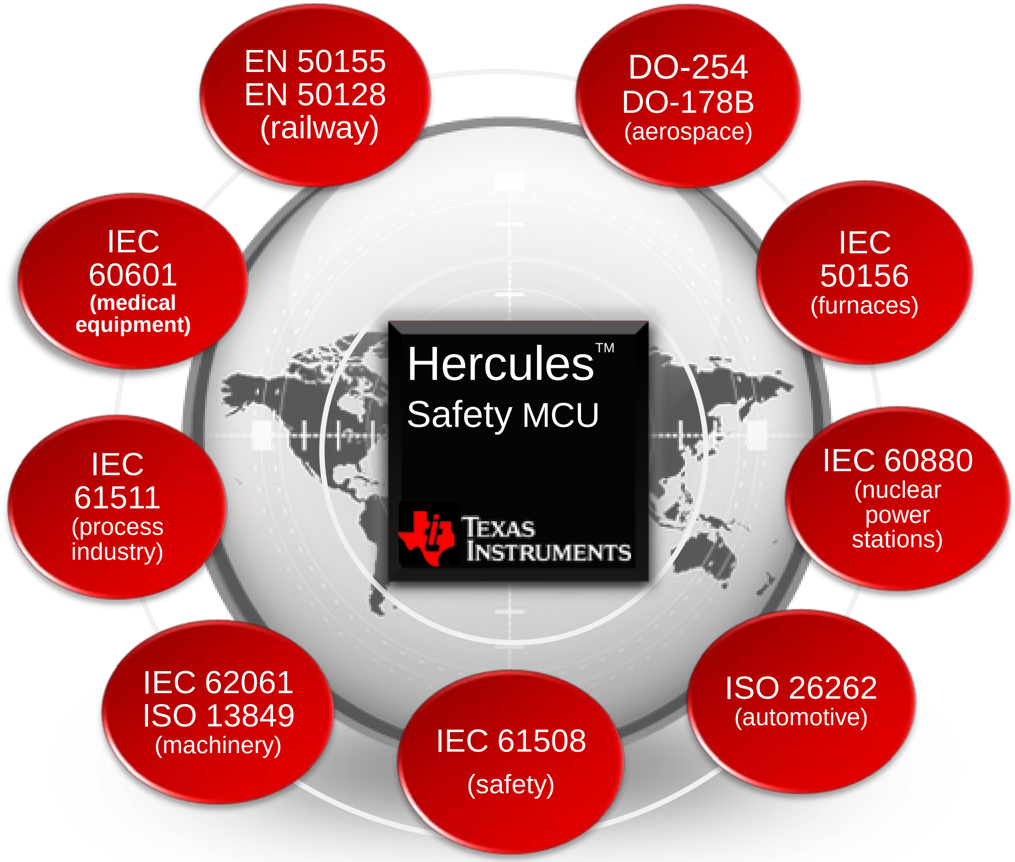
Active suspension, ABS, electric power steering, airbag and more!



Railway Systems



Anti-skid control



- Safety critical systems are everywhere
- Systems need to manage hazardous failures
- Many systems need to be safety-certified

Industrial and Medical



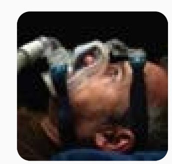
Sensor & communications gateway



Manufacturing, robotics, industrial automation, motor control



Wind Power



Anesthesia machines, respirators, ventilators, oxygen concentrators

Hercules™ MCU: End Equipment



TI Hercules™ MCU Platform

ARM® Cortex® Based Microcontrollers



Hercules™ MCU Platform

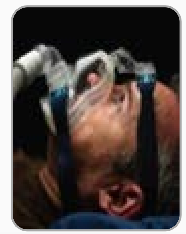


Lockstep MCUs for functional Safety

RM

Industrial and Medical Safety MCUs





- 80MHz to 330MHz
- 128KB to 4MB Flash
- -40 to 105°C Operation
- ENET, USB, CAN & UART
- Developed to Safety Standards
  - IEC 61508 SIL-3
- Cortex-R – up to 550 DMIPs

TMS570

Transportation and Automotive Safety MCUs





- 80MHz to 300MHz
- 128KB to 4MB Flash
- Automotive Q100 Qualification
- -40 to 125°C Operation
- FlexRay, ENET, CAN, LIN/UART
- Developed to Safety Standards
  - ISO 26262 ASIL-D
  - IEC 61508 SIL-3
- Cortex-R – up to 500 DMIPs

Hercules™ RM MCUs

Supporting Industrial & Medical safety

SafeTI™ Design Packages for Functional Safety

Benefits

- **Lockstep ARM Cortex-R based MCU –***with up to 550 peak DMIPS and 384KB to 4MB Flash Memory*
- **Safety Integrated in HW –** *provides a high level of diagnostic coverage to reduce safety software overhead*
- **SafeTI™ system design packages –** *makes it easier to achieve safety certification and get to market quickly*
- **Developed to safety standards –** developed for use in *IEC 61508 SIL-3 safety applications*
- **Flexible Communication and Control –** *Ethernet, USB, CAN. Up to 84 timer and 41 12-bit ADC channels.*

RMx

Temperatures	-40C	105C

ARM Cortex-R 80 to 330 MHz
- Cache (w/ECC)
- FPU
- MPU

Lockstep Fault Detection

Control
- ePWM
- eCAP
- eQEP
- N2HET Timer

Analog
- 12-bit 1 MSPS ADC
- Temperature Sensor

Memory
- Up to 4MB Flash (w/ ECC)
- Up to 512KB SRAM (w/ ECC)
- Up to 128KB Data Flash (w/ECC)

External Memory
- 16-bit Parallel Interface

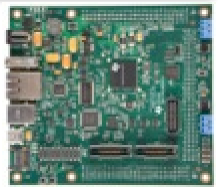
Communication
- 10/100 Ethernet
- USB
- CAN
- UART
- Multi-Buffer SPI
- I2C

Power & Clocking
- OSC PLL
- CLKMON
- VMON

Debug
- Real-time JTAG
- 32-bit Trace (ETM)
- Calibration

Safety & System
- CPU BIST
- SRAM BIST
- DMA
- CRC
- OS Timers
- Windowed Watchdog
- External INT / GPIO

Tools



Development Kit



Launchpad



XDS560 Pro Trace



SafeTI Kit

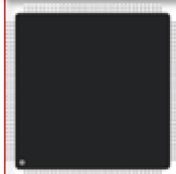


Motor Control

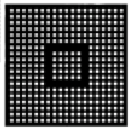
Software

- **Drivers & Libraries** – HALCoGen peripheral driver generation tool, SafeTI™ Diagnostic Library, CMSIS DSP Library
- **RTOS:** SAFERTOS, Codesys
- **IDEs:** Code Composer Studio, IAR
- **SafeTI Compiler Qualification Kit**
- **SafeTI 3rd Party Ecosystem**

Packages



144p QFP (20x20mm)
100p QFP (14x14mm)



337p BGA (16x16mm)

Hercules™ RM Cortex™-R Roadmap

2012

High

- **RM48L9x – 220MHz R4F**
  3MB Flash, 256kB RAM
  SafeTI ISO & IEC
- **RM48L5x – 200MHz R4F**
  2MB Flash, 192kB RAM
  SafeTI ISO & IEC

Features: SafeTI, Ethernet, USB, CAN

Low

Legend:
- Production
- Sampling
- Development

2013

Features:

- Lock Step Architecture
- QEP/PWM
- Ethernet
- CAN
- USB
- ISO 13849
- IEC 61508
- SafeTI

Mid

- **RM46L8x – 220MHz R4F**
  1.25MB Flash, 192kB RAM
  SafeTI ISO & IEC
- **RM46L4x – 200MHz R4F**
  1MB Flash, 128kB RAM
  SafeTI ISO & IEC

Features: SafeTI, Ethernet, USB, QEP/PWM, CAN

Low

- **RM42x – 100MHz R4**
  384kB Flash, 32kB RAM
  SafeTI ISO & IEC

Features: SafeTI, CAN

2014

High

- **RM57Lx – 330MHz R5F**
  4MB Flash, 512kB RAM

Features: Ethernet, QEP/PWM, CAN, SafeTI

Mid

- **Next Gen Mid**
  SafeTI ISO & IEC

Low

- **Next Gen Low**
  SafeTI ISO & IEC

Hercules™ TMS570 MCUs

SafeTI™ Design Packages for Functional Safety

Supporting Automotive & Transportation safety

Benefits

- **Lockstep ARM Cortex-R based MCU –***with up to 480 peak DMIPS and 256KB to 4MB Flash Memory*
- **Safety Integrated in HW –** *provides a high level of diagnostic coverage to reduce safety software overhead*
- **SafeTI™ system design packages –** *makes it easier to achieve safety certification and get to market quickly*
- **Developed to safety standards –** developed for use in *IEC 61508 SIL-3 and ISO 26262 ASIL-D safety applications*
- **Flexible Communication and Control –** *Ethernet, Flexray, CAN. Up to 84 timer and 41 12-bit ADC channels.*

TMS570x

Temperatures	-40C	125C	Q100

ARM Cortex-R 80 to 300 MHz
- Cache (w/ECC)
- FPU
- MPU

Lockstep Fault Detection

Control
- ePWM
- eCAP
- eQEP
- N2HET Timer

Analog
- 12-bit ADC
- Temperature Sensor

Memory
- Up to 4MB Flash (w/ ECC)
- Up to512KB SRAM (w/ ECC)
- 128KB Data Flash (w/ECC)

External Memory
- 16-bit Parallel Interface

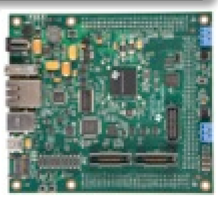
Communication
- 10/100 Ethernet
- CAN
- Flexray
- UART (LIN)
- Multi-Buffer SPI
- I2C

Power & Clocking
- OSC PLL
- CLKMON
- VMON

Debug
- Real-time JTAG
- 32-bit Trace (ETM)
- Calibration

Safety & System
- CPU BIST
- SRAM BIST
- DMA
- CRC
- OS Timers
- Windowed Watchdog
- External INT / GPIO

Tools



Development Kit



Launchpad



XDS560 Pro Trace



SafeTI Kit

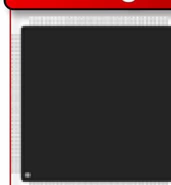


Motor Control

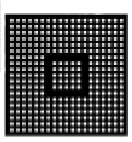
Software

- **Drivers & Libraries** – HALCoGen peripheral driver generation tool, SafeTI™ Diagnostic Library, CMSIS DSP Library,
- **RTOS –** SAFERTOS, AUTOSAR
- **IDEs:** Code Composer Studio, IAR
- **SafeTI Compiler Qualification Kit**
- **Mathworks Simulink**
- **SafeTI 3rd Party Ecosystem**

Packages



144p QFP (20x20mm)
100p QFP (14x14mm)



337p BGA (16x16mm)

Hercules™ TMS570 Cortex™-R Roadmap

	2012	2013	2014
High	**TMS570LS31x – 180MHz R4F** 3MB Flash, 256kB RAM **SafeTI ISO & IEC** **TMS570LS21x – 180MHz R4F** 2MB Flash, 192kB RAM **SafeTI ISO & IEC** CAN	**Features:** Lock Step Architecture QEP/ePWM Ethernet CAN CAN FlexRay ISO ISO 26262 IEC IEC 61508 SafeTI	**TMS570LC – 300MHz R5F** 4MB Flash, 512kB RAM CAN
Mid		**TMS570LS12x – 180MHz R4F** **1.25MB Flash, 192kB RAM** **SafeTI ISO & IEC** **TMS570LS11x – 180MHz R4F** **1MB Flash, 128kB RAM** **SafeTI ISO & IEC** CAN	**Next Gen Mid** **SafeTI ISO & IEC**
Low	Production Sampling Development	**TMS570LS04x – 80MHz R4** **384kB Flash, 32kB RAM** **SafeTI ISO & IEC** **TMS570LS03x – 80MHz R4** **256kB Flash, 24kB RAM** **SafeTI ISO & IEC** CAN	**Next Gen Low** **SafeTI ISO & IEC**

Texas Instruments

Functional Safety Standards Hardware requirements

Standard	System	Safety Integrity	Architectural Metric	Architectural Requirement	Failure Rate	Specific MCU self-test requirements
IEC 61508	Programmable E/E systems	SIL – 1,2,3,4	SFF	HFT>0 for SIL 4	PFD, PFH	No
ISO 26262	Automotive	ASIL – A, B, C, D	SPFM / LFM	No	PMHF	No
EN 50129	Railway	SIL- 1,2,3,4	N/A	Follow IEC 61508	THR	CPU, Memory
ISO 22201	Elevator	SIL – 1,2,3	N/A	Dual channels for SIL3	N/A	CPU, Memory, Interrupt, Clock, I/O, Comm
IEC 61800	Drive	SIL – 1,2,3 SIL4 Apply IEC 61508	SFF	Dependent on function	PFH (no PFD)	No
IEC 62061	Machinery	SIL – 1,2,3 SIL4 Apply IEC 61508	SFF	Supports ISO 13849 categories	PFH_D	No
IEC 61511	Process Automation	SIL – 1,2,3 SIL4 Apply IEC 61508	SFF	See IEC 61508	PFDavg	No
ISO 13849	Machinery	PL a,b,c,d,e	DC_{avg}	CAT B,1,2,3,4	$MTTF_D$	No
IEC 60730	Home Appliances	Class A, B, C	No	Yes (Class C)	No	CPU, Memory, Interrupt, Clock, I/O, Comms

Typical Usage of Hercules MCU per Functional Safety Standard*

Functional Safety Standard	Typical Hercules MCU Usage	Specific Diagnostic Requirements per Standard
IEC 61508	Single MCU for SIL1 - SIL 3, Dual MCU for SIL 4	No
ISO 26262	Single Hercules MCU ASIL A to D	No
EN 50129	Single MCU for SIL1 - SIL 3, Dual MCU for SIL 4	Examples provided, not requirements
ISO 22201	Single MCU for SIL1 - SIL 2, Dual MCU for SIL 3	Yes
IEC 61511	Single MCU for SIL1 - SIL 3, Dual MCU for SIL 4	No
IEC 61800	Single Hercules MCU for SIL1 - SIL 3	No
IEC 62061	Single Hercules MCU for SIL1 -SIL 3	No
ISO 13849	Single MCU for Cat B, 1, 2 from PL a to PLe Dual MCU for Cat 3, 4 from PL a to PL e Single MCU + TPS under evaluation for PL d CAT3	No
IEC 60730	Single MCU for Class A – C, Dual MCU for some Class C	Yes

* Items shown are typical examples. Achieved safety integrity level is the responsibility of the system developer.

Applying Functional Safety Standards

- **Functional Safety**
  - **Risk reduction**
    - **Safety Life Cycle**
      - Development Process
      - Safety Plan
      - Documentation
      - Config Management
      - Change Management
      - V&V
      - Personnel Competence
      - Certification
    - **SIL - 1/2/3/4**
      - Systematic Failures
        - Software
        - Tools
      - Random Failures
        - Diagnostics
        - Architectural Metric
        - Failure Rate

SafeTI™ Design Packages for Functional Safety

SafeTI™ design packages help meet functional safety requirements while managing both systematic and random failures.

系統失效

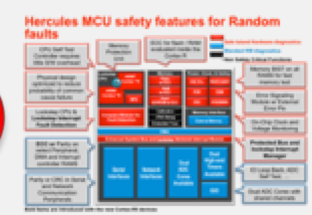
Process Certification
Software CSP
Compiler Qual. Kit





随机失效

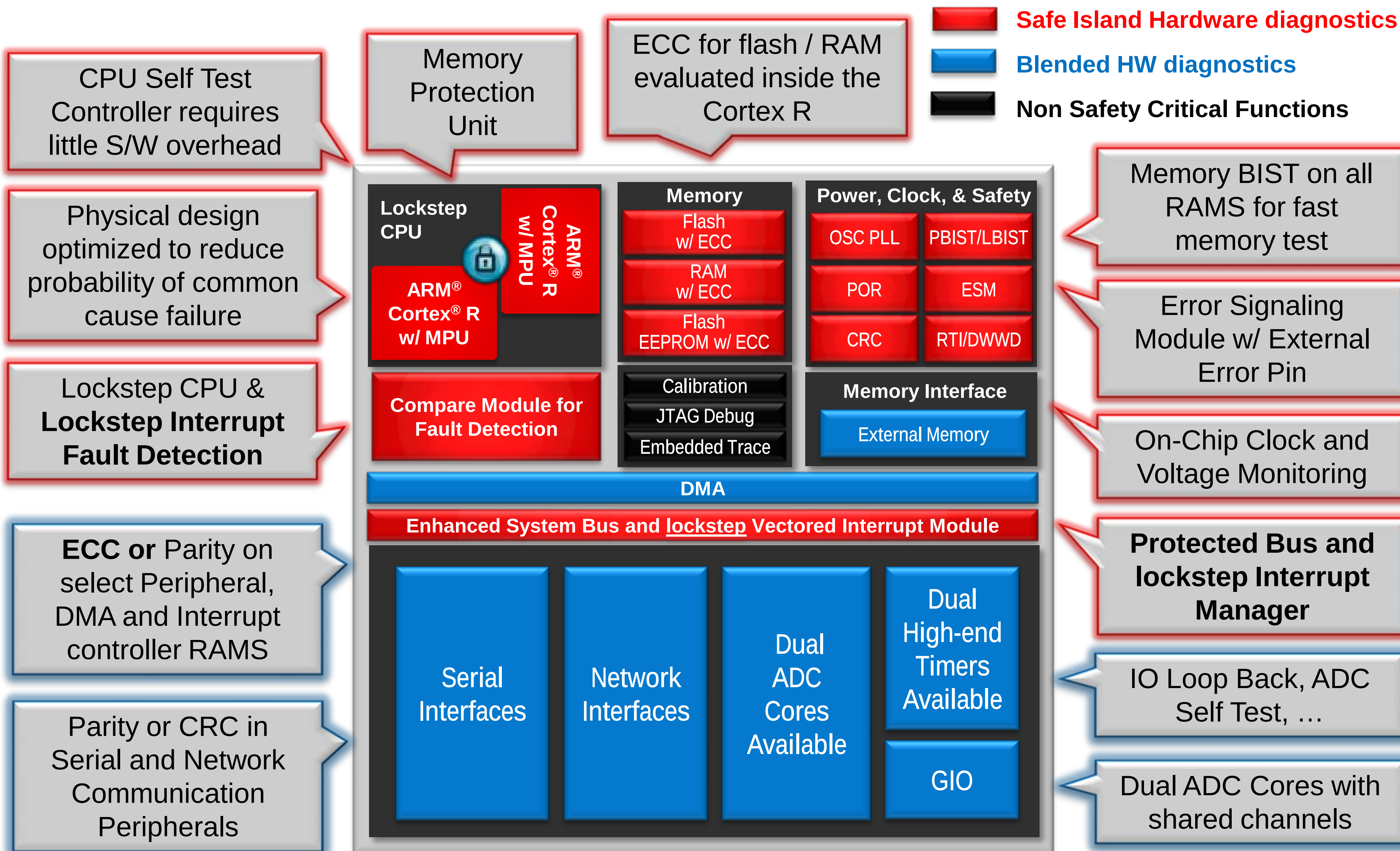
Hercules™ Architecture (FMEDA)



CSP = Compliance Support Package

Hercules™ MCU safety features

Random



Bold items are introduced with the new Cortex®-R5 devices

Hercules™ TMS570LS and RM4x Architecture Concept Assessment

Random

Technical Report

on the

Concept

of the

Hercules TMS570LSx and RM4x Platform Architecture

Manufacturer:

Texas Instruments Incorporated
12201Southwest Freeway
Stafford TX 77477
USA

Report no. TH854673T

Revision 1.0 of 2014-03-26

Test Laboratory

TÜV SÜD Rail GMBH
Generic Safety Systems
Barthstrasse 16
D-80339 Munich

2 Basis of Evaluation

The regulations and guidelines which form the basis of the type testing are listed below.

2.1 Functional Safety

No.	Standard	Title
[N1]	IEC 61508-2: 2010 (SIL 3)	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 2: Requirements for electrical/electronic/ programmable electronic safety-related systems
[N2]	ISO 26262-5:2011 (ASIL D)	Road vehicles — Functional safety — Part 5: Product development at the hardware level

Table 2: Functional Safety

5 Result of the concept review

5.1 Concept review based on IP-FMEAs

To evaluate the Platform Architecture according to the required failure modes defined in [N1] and [N2] for SIL 3 and ASIL D the analysis method Failure Mode and Effects Analysis (FMEA) was used. For each IP an own FMEA was created. Within these FMEAs diagnostic measures and timing aspects have been analysed. These FMEAs should be used in further development as input for the Safety requirement specification of several safety microcontroller devices.

Result:
The FMEAs provided in the documents [D1] - [D38] were made by Texas Instruments Incorporated and reviewed by TÜV SÜD. The results of the FMEAs meet the requirements according to [N1] and [N2]. These review results are recorded in [R1] - [R38]. The effectiveness of the selected diagnostic measures has to be verified on the final device.

6 Summary

For the analyzed failure modes according to [N1] - [N2] appropriate diagnostic measures to reach SIL 3 or ASIL D have been specified. A concluding re-evaluation of the IP-FMEAs has to be done in context of the final device.

SafeTI™ Hitex Safety Kit (SafeTI™- HSK)

Random





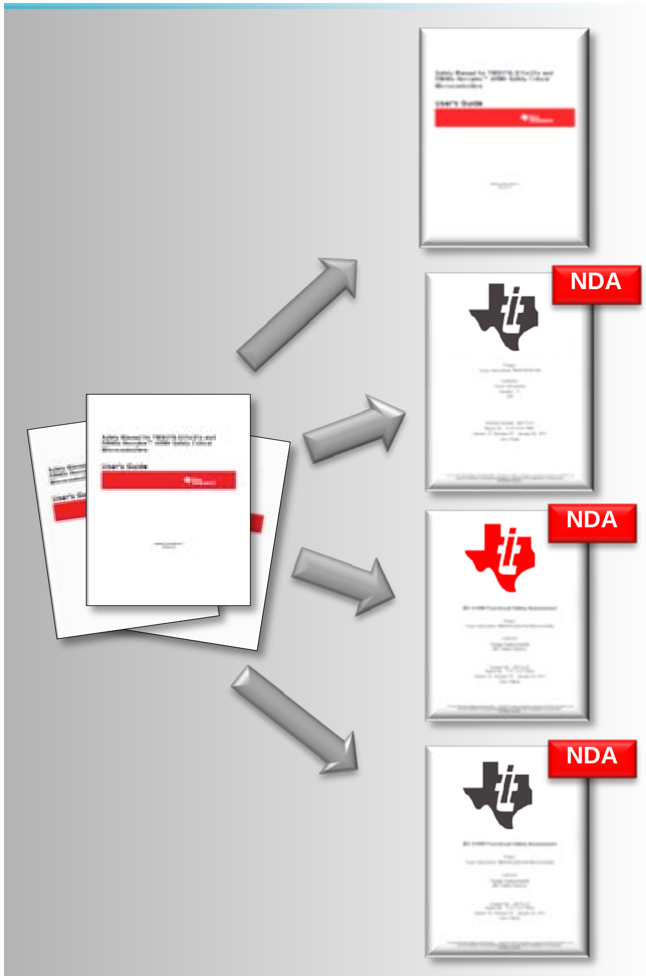


- Cost effective entry into functional safety related to ISO26262 and IEC61508
- Evaluate the use and performance of the Hercules™ MCU safety features
- Easily apply the recommendations of the Hercules™ MCU & TP 65381 Safety Manual
- Inject System & CPU faults and Monitor and Measure the reaction via a GUI
- Includes:
  - Evaluation Board with integrated debug, USB cable and Power Supply
  - Windows-based GUI
  - Demo Application with full source code
  - Code Composer Studio™ IDE
  - HALCogen and SafeTI Diagnostic Library
  - Evaluation version of SafeRTOS
  - User Manual

Hercules™ Safety Documents

Random

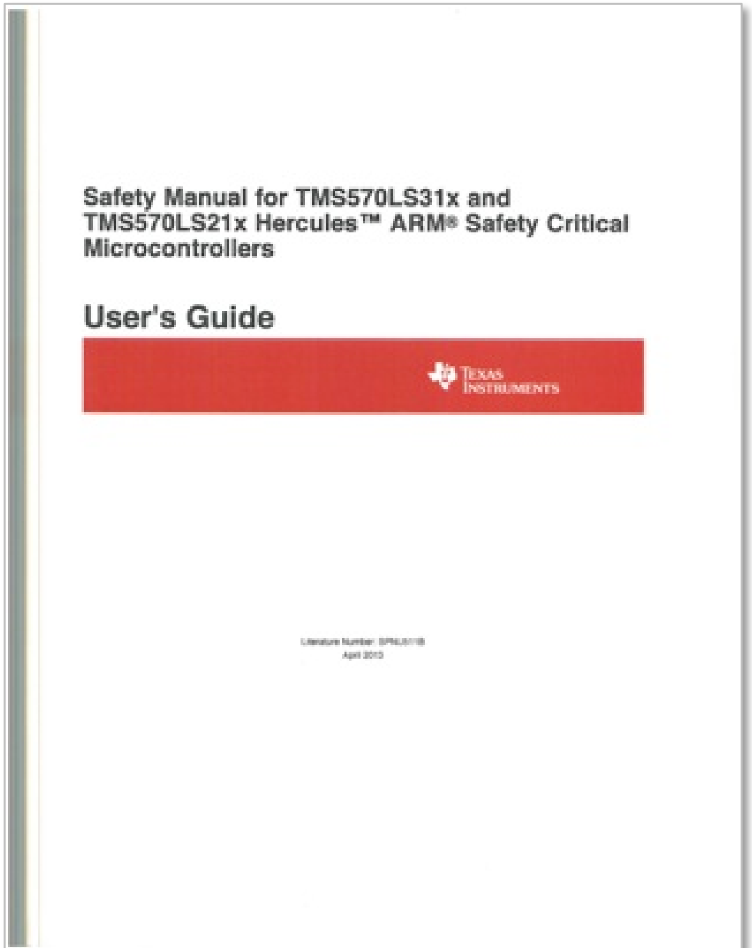
Documents provided by TI *some under NDA* to assist in the safety certification process:



- **Hercules™ component Safety Manual (SM)**
  Details product safety architecture and recommended usage
- **Safety Analysis Report Summary (SAR1)**
  Summary of FIT rate and FMEDA at component level for IEC 61508 and ISO 26262
- **Detailed Safety Analysis Report (SAR2)**
  - Full details of all safety analysis executed down to MODULE level for IEC 61508 and ISO 26262
  - Software tool for customizing analysis results to customer use case
- **Safety Report**
  Summary of compliance to IEC 61508 and/or ISO 26262

Hercules™ Safety Documents

Random



Safety Manual

- Summary of Development Flow
- Description of Safety Concept
- List of diagnostics
- List of assumptions

Table 2. Summary of Safety Features and Diagnostics

Device Partition	Unique Identifier	Safety Feature or Diagnostic	Feature Recommendation	Possible ISO 26262:2011 Latent Diagnostics
Power Supply	PWR1	Voltage monitor (VMON)	M	External Voltage Supervisor
	PWR2	External voltage supervisor	++	Voltage monitor (VMON)
Power Management Module (PMM)	PMM1	Lockstep PSCON	M	PSCON lockstep self test
	PMM2	Privileged mode access and multi-bit keys for control registers	M	Software test of register configuration and error response
	PMM3	Periodic software readback of static configuration registers	+	CPU lockstep
	PMM4	Software readback of written configuration	++	CPU lockstep
	PMM5	PSCON lockstep comparator self-test	++	Self-test autocoverage

Detailed Safety Analysis Reports

Random

Customer input for failure rate estimation

Package Used	TI PBGA
Customer input for transient fault estimation Application specific Flux Factor coeff. based on Jedec JESD89A	1
Maximum power dissipation Application specific power dissipation in Watts (0.934W is based on maximum datasheet value)	
Assumed Lifetime in years	
Confidence Level Desired confidence level of FIT rates	

Operational Profile from IEC/TR 62380:2004

	Temp1		Temp2		Temp3
	$(t_{ac})_1$ °C	τ1	$(t_{ac})_2$ °C	τ2	$(t_{ac})_3$
Profile	32	0.02	60	0.015	85

Safety mechanisms considered in the FMEDA

Device Partition	Unique identifier	Safety Feature or Diagnostic	Feature Reccomendation	Diagnostic Used in Application ?
Power Supply	PWR1	Voltage monitor (VMON)	M	1
Power Supply	PWR2	External voltage supervisor	++	1
Power Management Module (PMM)	PMM1	Lockstep PSCON	M	1
Power Management Module (PMM)	PMM2	Privileged Mode Access and Program Sequence Control Registers	M	1

Memory size

Type	Total Size	User Size	Unit
SRAM	256	256	Kbytes
FLASH	3	3	Mbytes
FLASH-FEE	64	64	Kbytes

Modules used for Safety Function / Safety

CPU SubSystem	Cortex R4F Central Processing Unit (	
CPU SubSystem	Vectored Interrupt Module (VIM)	
CPU SubSystem	LBIST	
CPU SubSystem	PBIST	
DEBUG	*Joint Technical Action Group (JTAG) D*	
DEBUG	*Cortex R4F Central Processing Unit (CF*	
DEBUG	*Data Modification Module*	
DEBUG	*Parameter Overlay Module*	
DEBUG	*RAM Trace Port*	
RAM System	SRAM and Level 1 (L1) Interconnect	
Flash System	One Time Programmable (OTP) Flas	
Flash System	Primary Flash and Level 1 (L1) Interc	
Flash System	Flash emulated EEPROM (FEE)	
INTERCONNECT	Level 2/Level 3 (L2/L3) Interconnect	
SYSTEM	Error Signaling Module (ESM)	
SYSTEM	Power Management Module (PMM)	
SYSTEM	Reset	
SYSTEM	System Control	
SYSTEM	Clock	
SYSTEM	EFuse Static Configuration	
SYSTEM	Direct Memory Access (DMA)	
SYSTEM	Input/Output (I/O) Multiplexing (IOMM)	YES
Peripheral	FlexRay Including FlexRay Transfer Unit (FTU)	YES

	Die Permanent	Die Transient	Package Permanent
Total FIT (Raw FIT)	9.24	724.99	71.82
Safety related FIT	9.23	722.00	71.82
Probabilistic Metrics for random Hardware Failures - PMHF (in FIT)	0.06	2.00	0.13
Single Point Fault Metric - SPFM	99.36%	99.72%	99.81%
Latent Fault Metric - LFM	99.98%	NA	99.81%

ISO 26262 categorization as in ISO 26262:2011-10, 8.1.8

		Die Permanent	Die Transient	Package Permanent
Total faults	λ	9.24	724.99	71.82
Total Safety Related faults	λ_{SR}	9.23	722.00	71.82
Total Not Safety Related faults	λ_{nSR}	0.00	2.98	0.00
Total Safe faults	λ_{S}	4.71	361.82	35.94
Total not Safe faults	λ_{nS}	4.53	360.18	35.94
Total faults with prob. of violate the SG	λ_{PVSG}	4.38	355.79	35.94
Total single point faults	λ_{SPF}	0.00	0.00	0.00
Total residual faults	λ_{RF}	0.06	2.00	0.13
Total Multi Point (ad)	$\lambda_{MPF}^{(ad)}$	0.14	NA	0.00
Total Multi Point (t)	$\lambda_{MPF}^{(t)}$	4.32	358.18	35.81
Total Multi Point detected faults	λ_{MPF_det}	4.46	NA	35.81
Total Multi Point latent faults	$\lambda_{MPF,l}$	0.00	0.00	0.00



- Adapt failure rate estimation model based on system usage
- Easily partition device into safety related and non-safety related functions
- Select applicable diagnostics from safety manual or apply your own diagnostics
- Automatic calculation of summarized and detailed ISO 26262 & IEC 61508 safety metrics

* FMEDA Developed with Yogitech

SafeTI™ Hardware Development Process Certification

Systematic



CERTIFICATE

No. Q4B 13 03 84071 001

Holder of Certificate: Texas Instruments Incorporated
12201 Southwest Freeway
Stafford TX 77477
USA

Factory(ies): Texas Instruments Incorporated
12201 Southwest Freeway, Stafford TX 77477, USA

Texas Instruments Deutschland GmbH
Haggertystr. 1, 85356 Freising, GERMANY

Certification Mark:

Scope of Certificate: QRAS AP00210

Applied Standard(s): IEC 61508-1:2010
IEC 61508-2:2010
ISO 26262-2:2011
ISO 26262-5:2011

The Certification Body of TÜV SÜD Product Service GmbH certifies that the company mentioned above has established and is maintaining a management system which meets the requirements of the listed standards. The results are documented in a report. See also notes overleaf.

Report No.: TF84823T

Valid until: 2016-03-07

Date, 2013-03-12 (Guido Neumann)

Page 1 of 1

TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstraße 65 · 80339 München · Germany

TI's hardware functional safety development process has been certified for:

- ➢ IEC 61508 SIL-3
- ➢ ISO 26262 ASIL-D

The certification demonstrates TI's commitment to have a process suitable for developing hardware components that are compliant to ISO 26262 and IEC 61508

Hercules™ and SafeTI™ Software and Tool Packages

Systematic

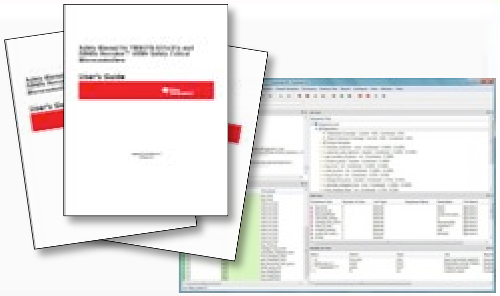
Hercules Software and Tools

- ❑ Production quality software to easily use Hercules MCU
- ❑ Includes GUI configurator (where relevant)
- ❑ Includes User Guide and Release Notes



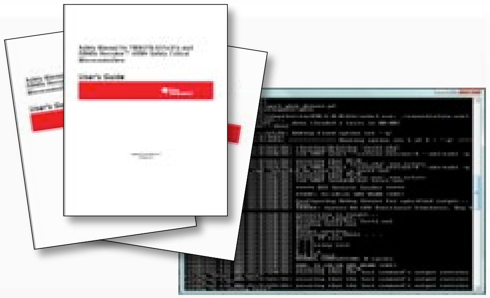
SafeTI Compliance Support Package

- ❑ Provide evidence to safety standards
- ❑ Includes Test Reports, Quality Metrics, Safety Manual, etc.
- ❑ Software developed to IEC 61508 & ISO 26262 requirements



SafeTI Tool Qualification Kit

- ❑ Assists in qualifying the TI ARM Compiler to functional safety standards
- ❑ Model-based tool qualification methodology
- ❑ Assessed to comply with both IEC 61508 and ISO 26262



SafeTI™ Compiler Qualification Kit

Systematic



- Assists in qualifying the TI ARM C/C++ Compiler to functional safety standards
- Qualification of customer specific use case can be less restrictive than certified compilers
- Application of kit assessed by TÜV Nord to comply with both IEC 61508 and ISO 26262
- Includes:
  - Qualification Support Tool (model-based)
  - Process specific documentation:
    - Tool Classification Report
    - Tool Qualification Plan
    - Tool Qualification Report
    - Tool Safety Manual
  - ACE SuperTest™ qualification suite
  - TI compiler validation test cases
  - Test Automation Unit (TAU)
  - 24hrs of Validas consulting services
  - TÜV Nord assessment report

Approved by TÜV NORD

Agenda

- Overview of Hercules™ MCU and SafeTI™ Design package
- Hercules™ MCU Functional Safety How-To Workshop
  - Safety Functions, Safety Goals, Safe State, SIL, Failure rate
  - Safety Critical Elements identification and Diagnostic Requirements
  - Safety Manual and Diagnostics Selection
  - Mission Profile and Failure Rate Estimation
  - SafeTI™ Diagnostic Library
  - SafeTI™ Diagnostic Library Compliance Support Package (CSP) certification support
  - Fault Injection with HITEX kit
- Summary

Applying Functional Safety Standards

SafeTI™ Design Packages for Functional Safety

- Functional Safety
  - Risk reduction
    - Safety Life Cycle
      - Development Process
      - Safety Plan
      - Documentation
      - Config Management
      - Change Management
      - V&V
      - Personnel Competence
      - Certification
    - SIL - 1/2/3/4
      - Systematic Failures
        - Software
        - Tools
      - Random Failures
        - Diagnostics
        - Architectural Metric
        - Failure Rate

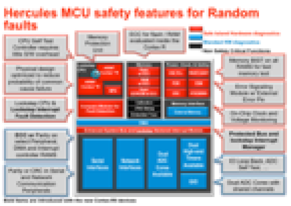
SafeTI™ design packages help meet functional safety requirements while managing both systematic and random failures.

Workshop will address:

- How to manage MCU hardware random failures
- How to estimate failure rate vs SIL requirements
- Software support



Hercules™ Architecture (FMEDA)

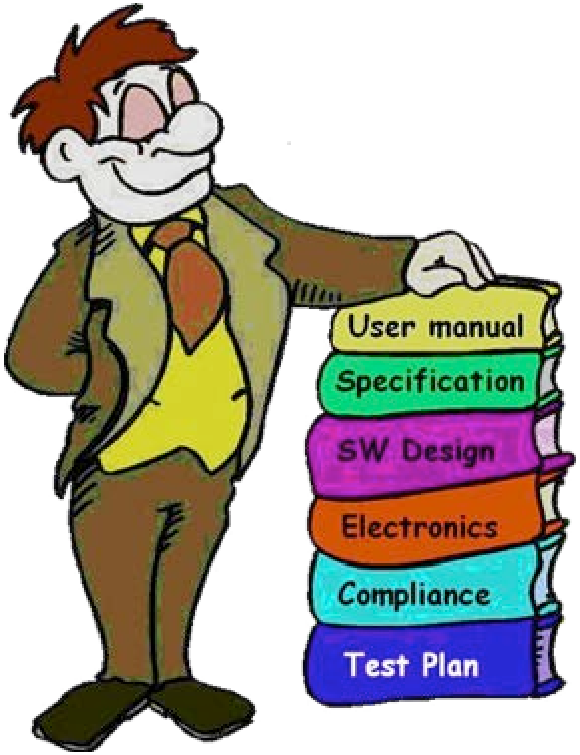


CSP = Compliance Support Package

Functional Safety Certification

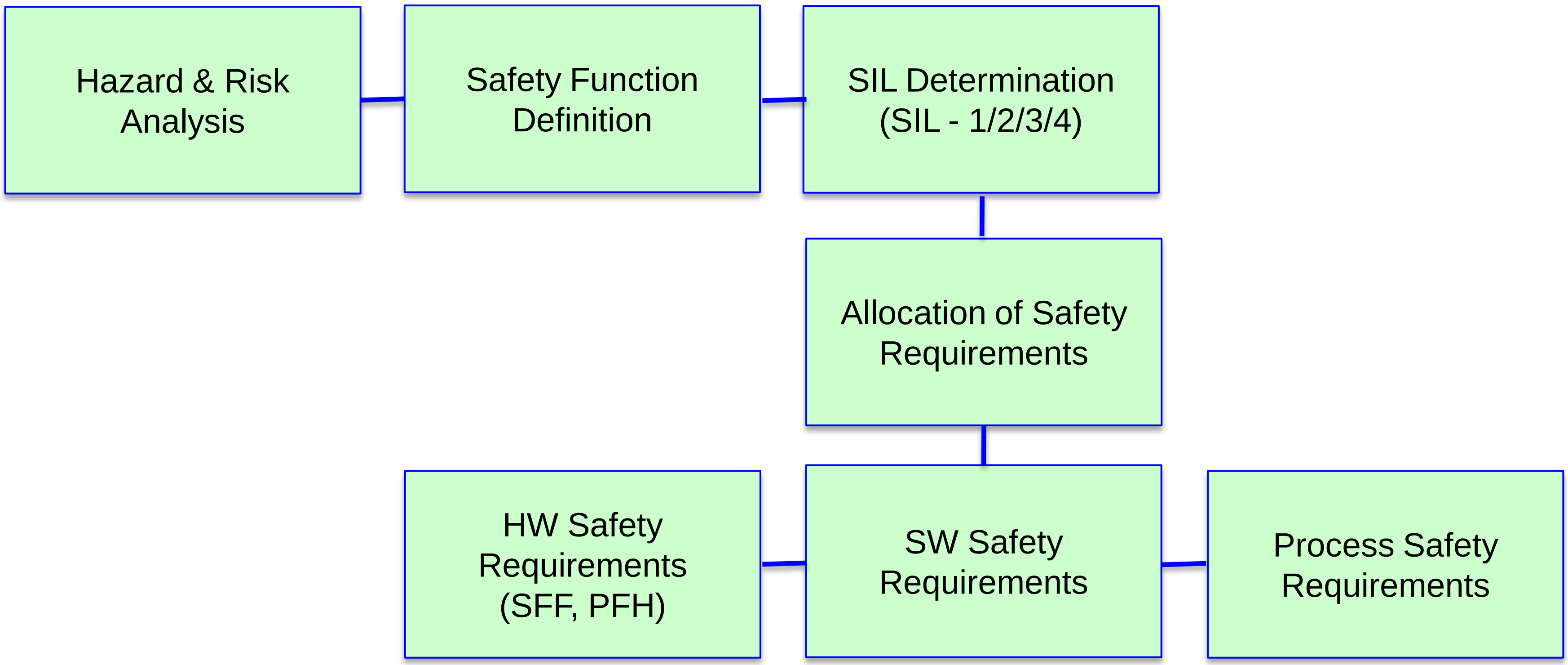
System

Development Process	Software	Hardware
MCU Development Process	MCU Software Drivers, Library Tool	MCU Hardware Architecture Failure rate

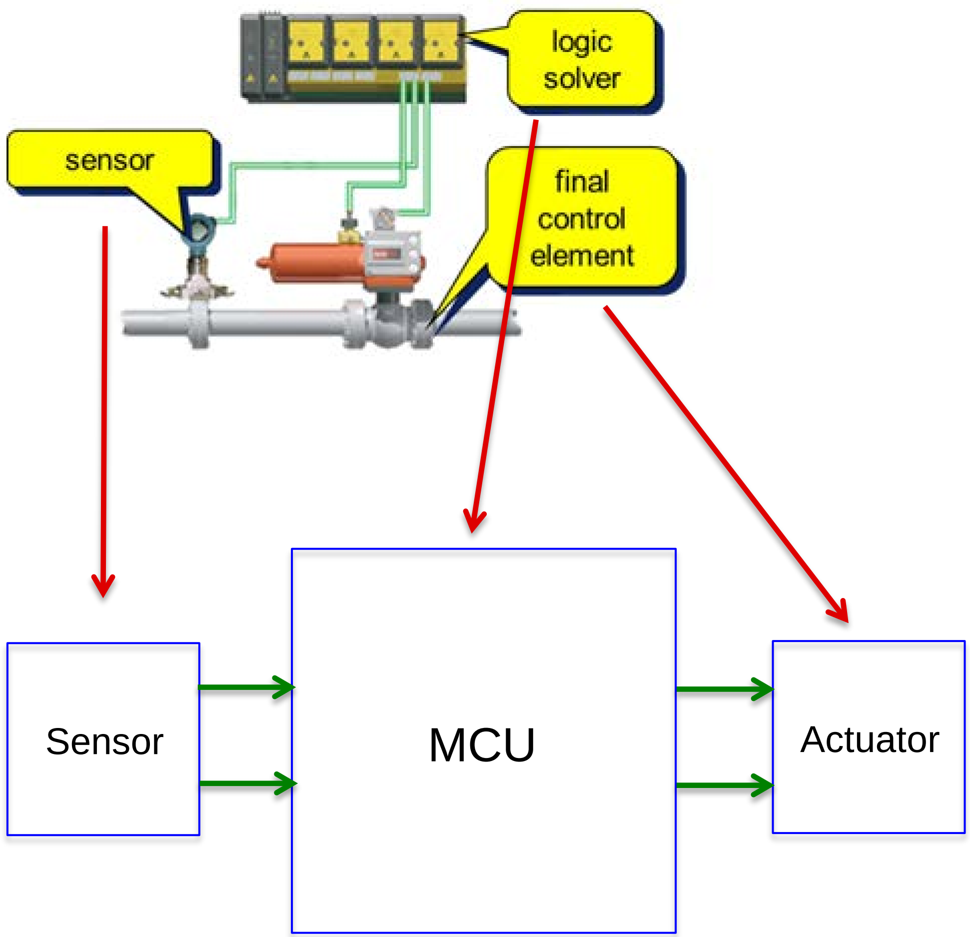


Show me evidence

IEC 61508
Hazard/Risk Analysis & SIL determination



Safety Function / Safe State

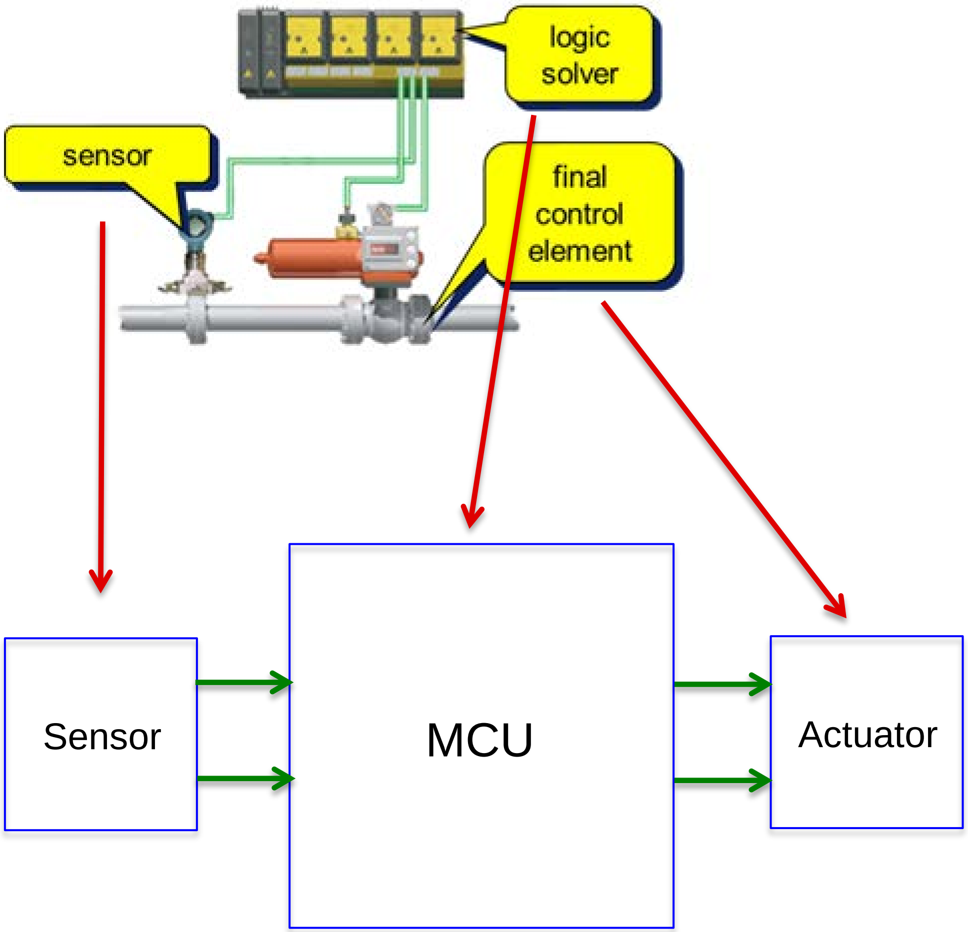


Hazard analysis -> Safety Function & Safe State

Safety Function: function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the ECU, in respect of a specific hazardous event

Safe State: State of the ECU when safety is achieved

Safety Function / Safe State



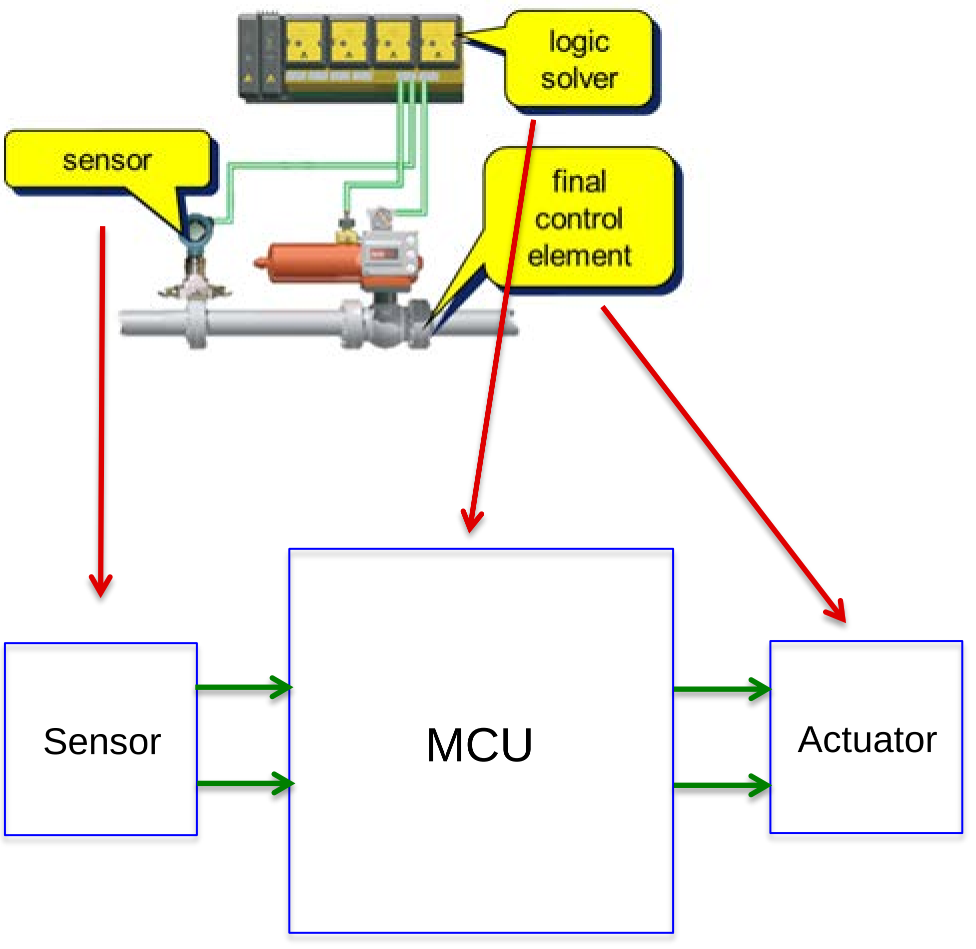
Hazard: High gas flow pressure

Safety Function: Monitor the pressure of gas flow.

Safe State:

1. If gas flow pressure exceeds a fixed limit, shut off the gas flow valve.
2. If a dangerous fault is detected in the system, shut off the gas flow

Risk Analysis / Safety Integrity Level

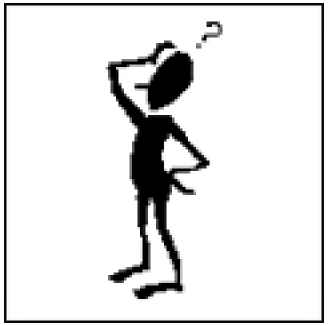


<u>Risk Analysis</u> determines the performance requirement of the safety function, i.e. **<u>SIL level</u>** and how much risk reduction?

<u>Safety Integrity Level</u> (SIL 1/2/3/4) is determined by the consequence and the frequency of hazardous event. The higher the SIL level, the higher the risk reduction requirements

Safety Integrity Level

- Safety Integrity Level is characterized by SFF and PFD_{AVG} or PFH
  - Single Failure Fraction (SFF)
  - Probability of Fail on Demand Average (PFD_{AVG})
  - Probability of Fail per Hour (PFH)
- $SFF = (\lambda_{SAFE} + \lambda_{DANGEROUS\text{-}DETECTED}) / (\lambda_{SAFE} + \lambda_{DANGEROUS\text{-}DETECTED} + \lambda_{DANGEROUS\text{-}UNDETECTED})$
- $PFH \approx 1 / \lambda_{DANGEROUS\text{-}UNDETECTED}$



How to calculate all these?

Safety Integrity Level

Table 2 – Safety integrity levels – target failure measures for a safety function operating in low demand mode of operation

Safety integrity level (SIL)	Average probability of a dangerous failure on demand of the safety function (PFD_{avg})
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Low demand functions have less stringent requirements on PFDavg to achieve a specific SIL.

Table 3 – Safety integrity levels – target failure measures for a safety function operating in high demand mode of operation or continuous mode of operation

Safety integrity level (SIL)	Average frequency of a dangerous failure of the safety function [h^{-1}] (PFH)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

High demand and continuous demand functions have more stringent requirements on PFH to achieve a specific SIL.

Table 3 – Maximum allowable safety integrity level for a safety function carried out by a type B safety-related element or subsystem

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
<60 %	Not Allowed	SIL 1	SIL 2
60 % – <90 %	SIL 1	SIL 2	SIL 3
90 % – <99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Type B products are complex products in which all failure modes are not known. Most semiconductors are considered Type B.

HFT = Hardware Fault Tolerance where 0=No redundancy

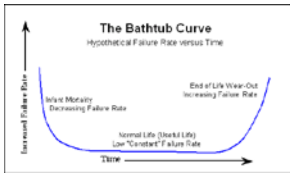
Maximum Allowable SIL for Type B (High Demand) Systems
IEC61508-2 Table 3

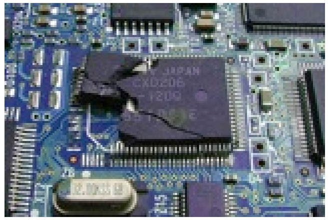
Safe Failure Fraction of an Element (SFF)	Hardware Fault Tolerance		
	0	1	2
<60%	Not Allowed	SIL1	SIL2
60% - <90%	SIL1	SIL2	SIL3
90% - <99%	SIL2	SIL3	SIL4
>99%	SIL3	SIL4	SIL4

SIL	SFF (HFT=0)	PFH (FIT)
SIL1	0% … <60%	<10000
SIL2	60% … <90%	<1000
SIL3	90% … <99%	<100

1 FIT = 1 failure in 1E9 hours

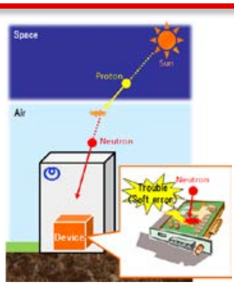
MCU Failure Mode and Failure Rate

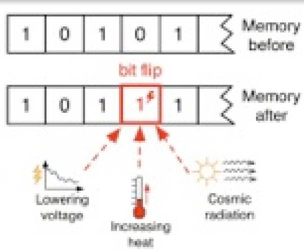




- **<u>Permanent random failures:</u>**
  - Tox integrity, Short, Open, Stuck At, Drift ….

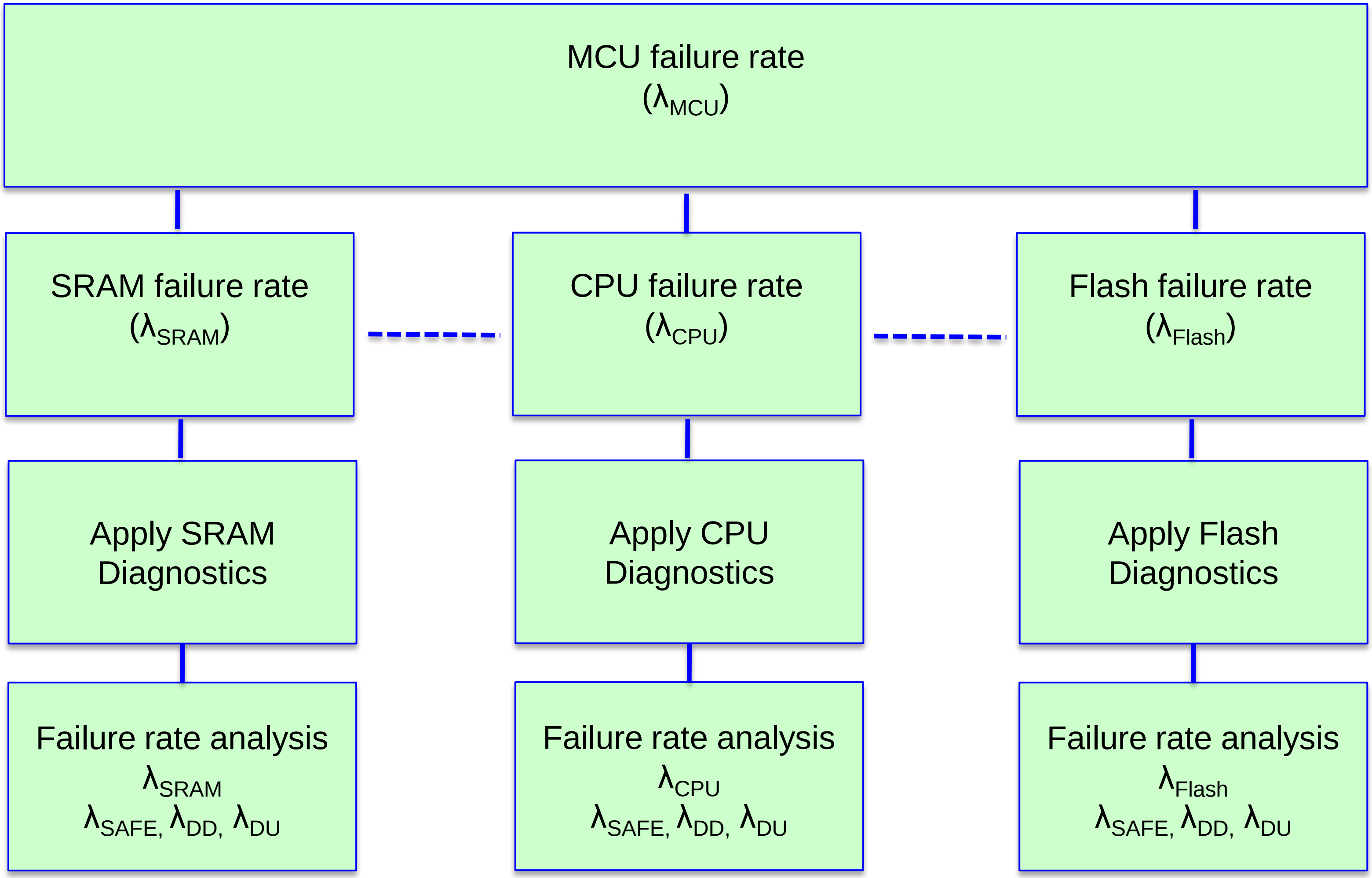
- Source of permanent component failure rate data:
  - MILHDBK 217F
  - SN29500
  - IEC/TR 62380
  - Supplier reliability data
  - …
- TI uses IEC/TR 62380 where # of transistors, # of memory bits, temperature and package effect can be modeled.
- Failure rate is commonly expressed in FIT (Failure In Time)
  - 1 FIT = 1 failure in 1E9 hours.





- **<u>Transient random failures:</u>**
  - Cosmic Rays, EMC
- Failure rate data source is TI experiments in Los Alamos lab and TI lab

MCU Failure Rate Estimation



Apply diagnostics to detect dangerous faults until appropriate SIL metrics (SFF, PFH) are met

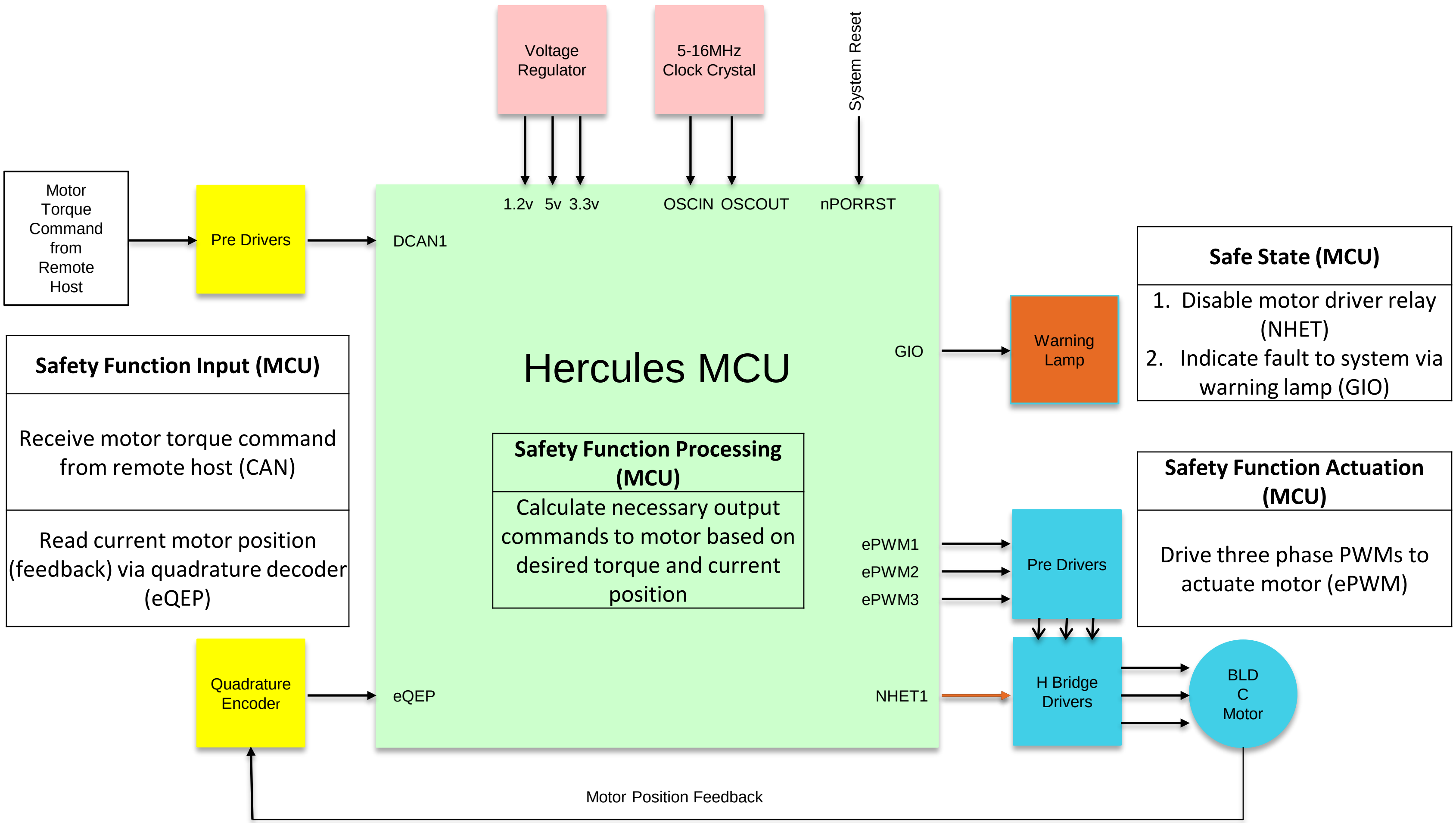
λ_{SAFE} - Safe, λ_{DD} – Dangerous Detected, λ_{DU} – Dangerous Undetected

Agenda

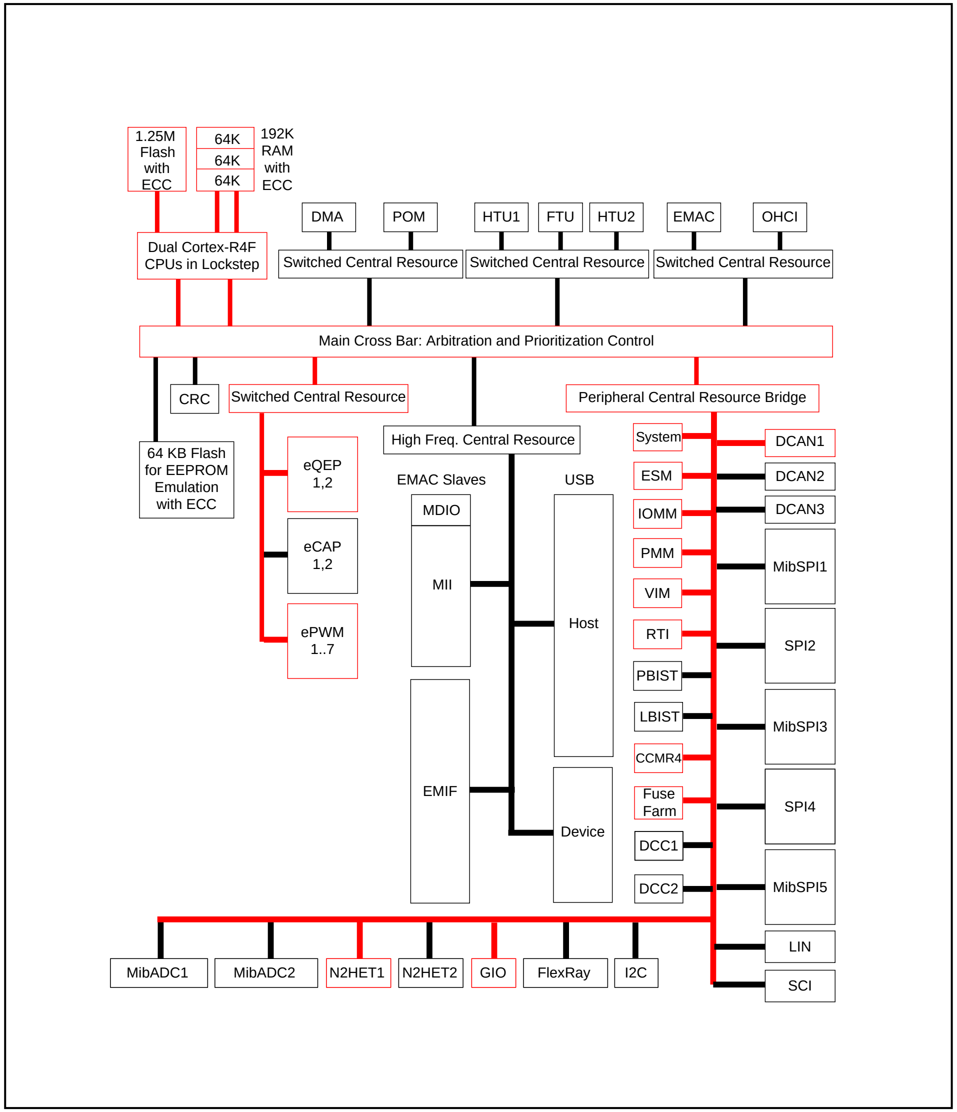
- Overview of Hercules^{TM} MCU and SafeTI^{TM} Design package
- Hercules^{TM} MCU Functional Safety How-To Workshop
  - Safety Functions, Safety Goals, Safe State, SIL, Failure rate
  - Safety Critical Elements identification and Diagnostic Requirements
  - Safety Manual and Diagnostics Selection
  - Mission Profile and Failure Rate Estimation
  - SafeTI^{TM} Diagnostic Library
  - SafeTI^{TM} Diagnostic Library Compliance Support Package (CSP) certification support
  - Fault Injection with HITEX kit
- Summary

Application Example

Safety Goal: The motor shall deliver torque as commanded by the external host.



MCU Safety Critical Elements per Safety Function

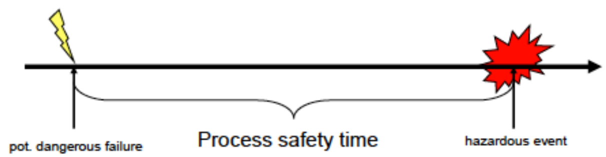


- Safety Critical Elements are elements within MCU the implement the safety function
- Diagnostics are necessary to detect safety related failures
- Sufficient diagnostics coverage (DC) is needed to meet required IEC 61508 HW metrics per SIL level
- In this example, safety critical elements are: CPU, Flash, SRAM, Interconnect, eQEP, eCAP, ePWM, System, ESM… I2C

Safety Function Definition

Safety Function ID	Equivalent Safety Goal ID	Safety Function Input (MCU)	Safety Function Processing (MCU)	Safety Function Actuation (MCU)
SF_1	SG_1	Receive motor torque command from remote host (CAN) Read current motor position (feedback) via quadrature decoder (eQEP)	Calculate necessary output commands to motor based on desired torque and current position	Drive three phase PWMs to actuate motor (ePWM)

- Process safety time (PST):
  - time between occurrence of a potential dangerous failure and the hazardous event



Equivalent Safety Goal	Safe State (MCU)
The motor shall deliver torque as commanded by the external host.	1. Disable motor driver relay (NHET) 2. Indicate fault to system via warning lamp (GIO)

SIL		Equivalent FTTI
3	10ms	10 ms

MCU Safety Diagnostic Requirements
per Safety Function

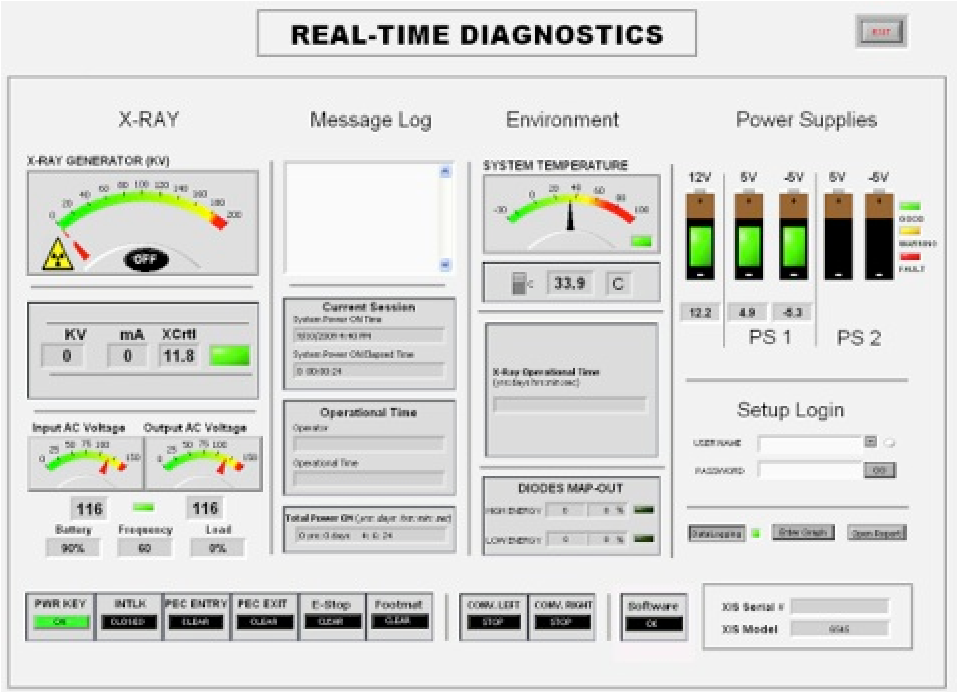
Safety Requirement ID	Satisfies	Assumed Safety Diagnostic Requirement	SIL
SFR_1	SF_1	MCU safety related functional input shall be considered safety critical	SIL 3
SFR_1.1	SFR_1	DCAN1 shall be considered safety critical	SIL 3
SFR_1.2	SFR_1	eQEP1 shall be considered safety critical	SIL 3
SFR_2	SF_1	MCU safety related functional output shall be considered safety critical	SIL 3
SFR_2.1	SFR_2	ePWM1 shall be considered safety critical	SIL 3
SFR_2.2	SFR_2	ePWM2 shall be considered safety critical	SIL 3
SFR_2.3	SFR_2	ePWM3 shall be considered safety critical	SIL 3
SFR_3	SF_1	MCU safety related processing shall be considered safety critical	SIL 3
SFR_3.1	SFR_3	Cortex R4F CPU shall be considered safety critical	SIL 3
SFR_3.2	SFR_3	TCM SRAM as needed to support the application shall be considered safety critical	SIL 3
SFR_3.3	SFR_3	TCM Flash as needed to support the application shall be considered safety critical	SIL 3
SFR_3.4	SFR_3	L2/L3 interconnect as needed to support the application shall be considered safety critical	SIL 3
SFR_3.5	SFR_3	VIM shall be considered safety critical	SIL 3
SFR_4	SF_1	MCU functions necessary to support safety related input, processing, and output shall be considered safety critical	SIL 3
SFR_4.1	SFR_4	Power supply shall be considered safety critical	SIL 3
SFR_4.2	SFR_4	PMM shall be considered safety critical	SIL 3
SFR_4.3	SFR_4	Clocking subsystem shall be considered safety critical	SIL 3
SFR_4.4	SFR_4	Reset logic shall be considered safety critical	SIL 3
SFR_4.5	SFR_4	I/O multiplexing (IOMM) shall be considered safety critical	SIL 3
SFR_4.6	SFR_4	RTI shall be considered safety critical	SIL 3
SFR_4.7	SFR_4	System control module shall be considered safety critical	SIL 3
SFR_4.8	SFR_4	ESM shall be considered safety critical	SIL 3
SFR_4.9	SFR_4	Fuse Farm shall be considered safety critical	SIL 3
SFR_4.10	SFR_4	OTP configuration shall be considered safety critical	SIL 3
SFR_5	SF_1	MCU functions necessary to support the safe state shall be considered safety critical	SIL 3
SFR_5.1	SFR_5	NHET1 shall be considered safety critical	SIL 3
SFR_5.2	SFR_5	GIO shall be considered safety critical	SIL 3

MCU Diagnostic Tests



Start up diagnostics examples

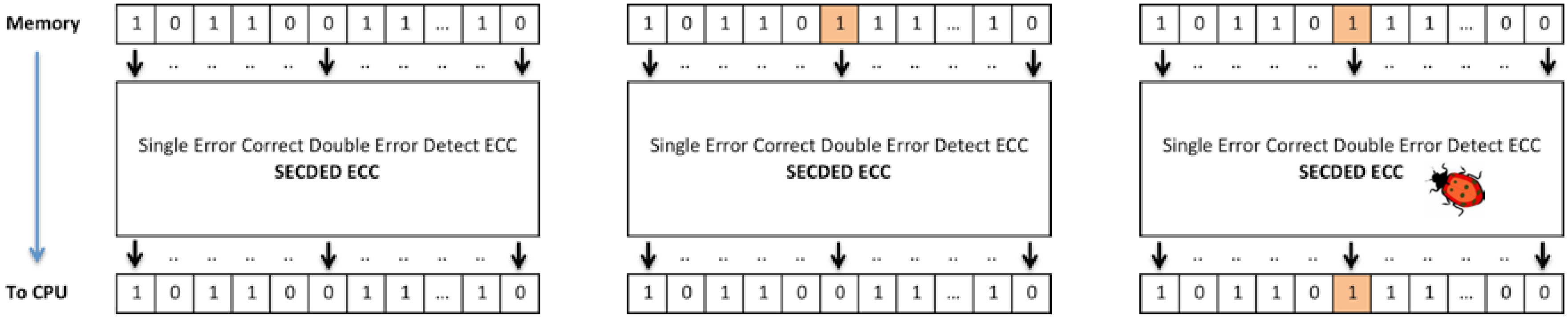
- SRAM self test
- CPU self test
- ADC self test
- I/O loop back



Real-time diagnostics examples

- SRAM/Flash ECC
- CPU compare
- Clock monitor
- Power monitor
- MPU

What is Latent Diagnostics? Why it is important?



- Memory content OK
- No error detected by ECC
- Read to CPU OK

- Memory single bit error
- Error detected & corrected by ECC
- Read to CPU OK

- Memory single bit error
- Error NOT detected & corrected by ECC
- Read to CPU NOT OK

The bug in the ECC block will only violate the safety goal IN COMBINATION with a memory fault -> a latent fault

<u>Need to test the diagnostic circuits such as ECC, Lock-Step Compare</u>

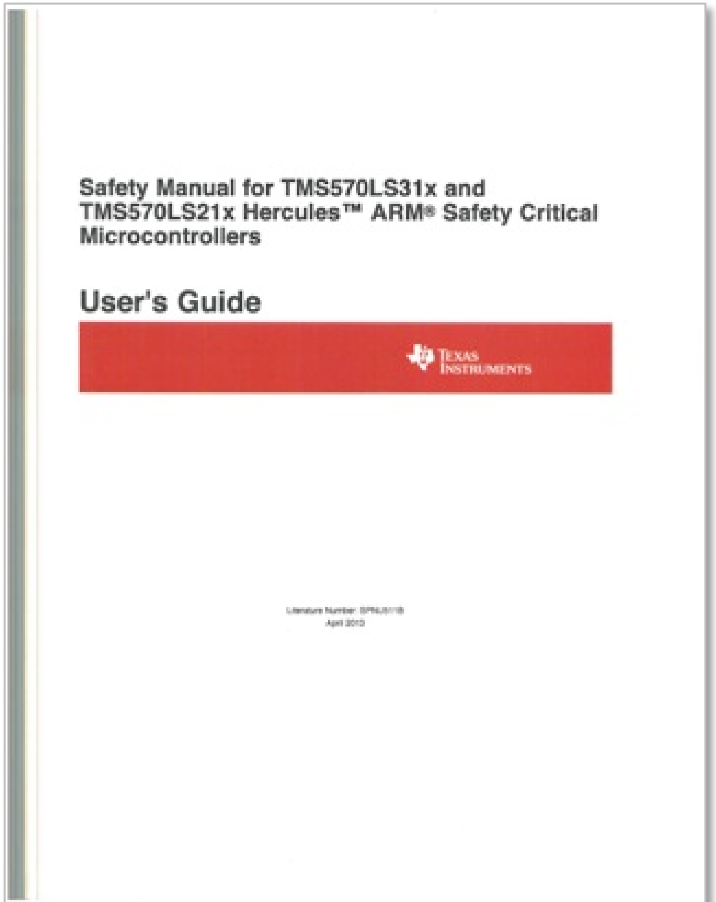
Agenda

- Overview of Hercules™ MCU and SafeTI™ Design package
- Hercules™ MCU Functional Safety How-To Workshop
  - Safety Functions, Safety Goals, Safe State, SIL, Failure rate
  - Safety Critical Elements identification and Diagnostic Requirements
  - Safety Manual and Diagnostics Selection
  - Mission Profile and Failure Rate Estimation
  - SafeTI™ Diagnostic Library
  - SafeTI™I Diagnostic Library Compliance Support Package (CSP) certification support
  - Fault Injection with HITEX kit
- Summary

How to implement Diagnostics?

INFO
SAFETY MANUAL

Hercules™ Safety Manual


Safety Manual for TMS570LS31x and TMS570LS21x Hercules™ ARM® Safety Critical Microcontrollers

User's Guide

Texas Instruments

Table 2. Summary of Safety Features and Diagnostics

Device Partition	Unique Identifier	Safety Feature or Diagnostic	Feature Recommendation	Possible ISO 26262:2011 Latent Diagnostics
Power Supply	PWR1	Voltage monitor (VMON)	M	External Voltage Supervisor
	PWR2	External voltage supervisor	++	Voltage monitor (VMON)
Power Management Module (PMM)	PMM1	Lockstep PSCON	M	PSCON lockstep self test
	PMM2	Privileged mode access and multi-bit keys for control registers	M	Software test of register configuration and error response
	PMM3	Periodic software readback of static configuration registers	+	CPU lockstep
	PMM4	Software readback of written configuration	++	CPU lockstep
	PMM5	PSCON lockstep comparator self-test	++	Self-test autocoverage

- An overview of the safety architecture for management of random failures
- The details of architecture partitions, implemented safety mechanisms, and recommended usage
- Failure modes and failure rates

IEC61508 HW Metrics Calculation Select Safety Features - CPU

From Safety Manual				
Device Partition	**Unique identifier**	**Safety Feature or Diagnostic**	**Feature Reccomendation**	**Diagnostic Used in Application?**
Cortex R4F Central Processing Unit (CPU)	CPU1	Lockstep compare	M	1
Cortex R4F Central Processing Unit (CPU)	CPU2A	Boot time execution of LBIST STC	++	1
Cortex R4F Central Processing Unit (CPU)	CPU2B	Periodic execution of LBIST STC	O	0
Cortex R4F Central Processing Unit (CPU)	CPU3	MPU	++	1
Cortex R4F Central Processing Unit (CPU)	CPU4	Online profiling using PMU	O	0
Cortex R4F Central Processing Unit (CPU)	CPU5A	Internal watchdog -DWD	O	0
Cortex R4F Central Processing Unit (CPU)	CPU5B	Internal watchdog -DWDD	O	0
Cortex R4F Central Processing Unit (CPU)	CPU5C	External watchdog	+	1
Cortex R4F Central Processing Unit (CPU)	CPU6	Illegal operation and instruction trapping	++	1
Cortex R4F Central Processing Unit (CPU)	CPU7	SW readback of written configuration	++	1
Cortex R4F Central Processing Unit (CPU)	CPU8	Lockstep compare (CCM) self-test	++	1

- Safety Mechanisms associated with CPU are selected.
  - ‘1’ means the safety mechanism is assumed in the HW metrics calculation
  - ‘0’ means not assumed

Based on RM42x/LS04x/LS03x v0.8 FMEDA worksheet

Cortex-R: Ideal for safety critical applications

Safety features

- ❑ Supports Lockstep
- ❑ Memory Protection Unit (MPU)
- ❑ Error-Correcting Code (ECC)

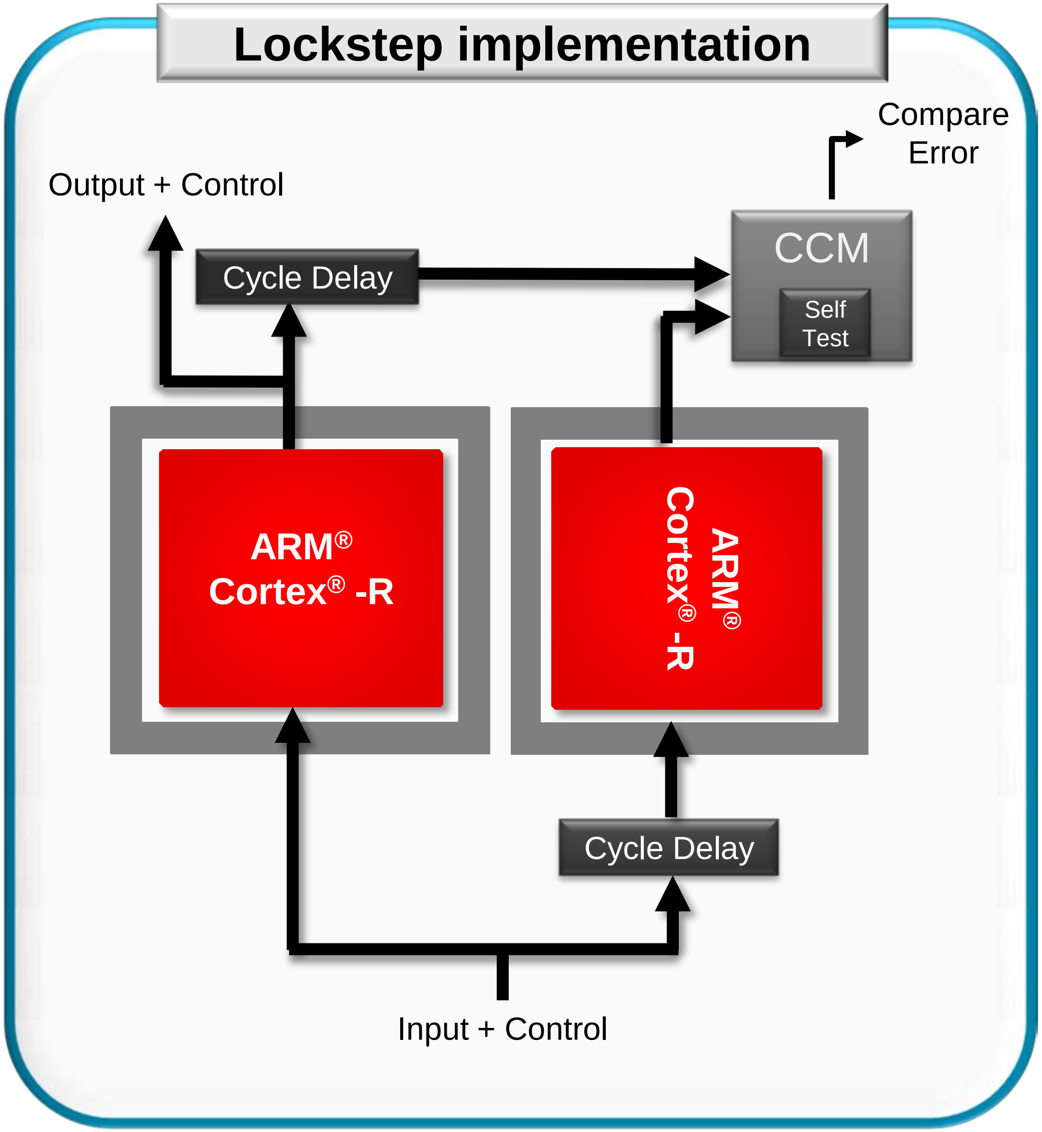
Higher performance

- ❑ 8-stage processor pipeline
- ❑ Dual issue – two instructions can execute in parallel
- ❑ Load store unit reduces stalling
- ❑ Pre-fetch and Branch Prediction Units
- ❑ Cached*

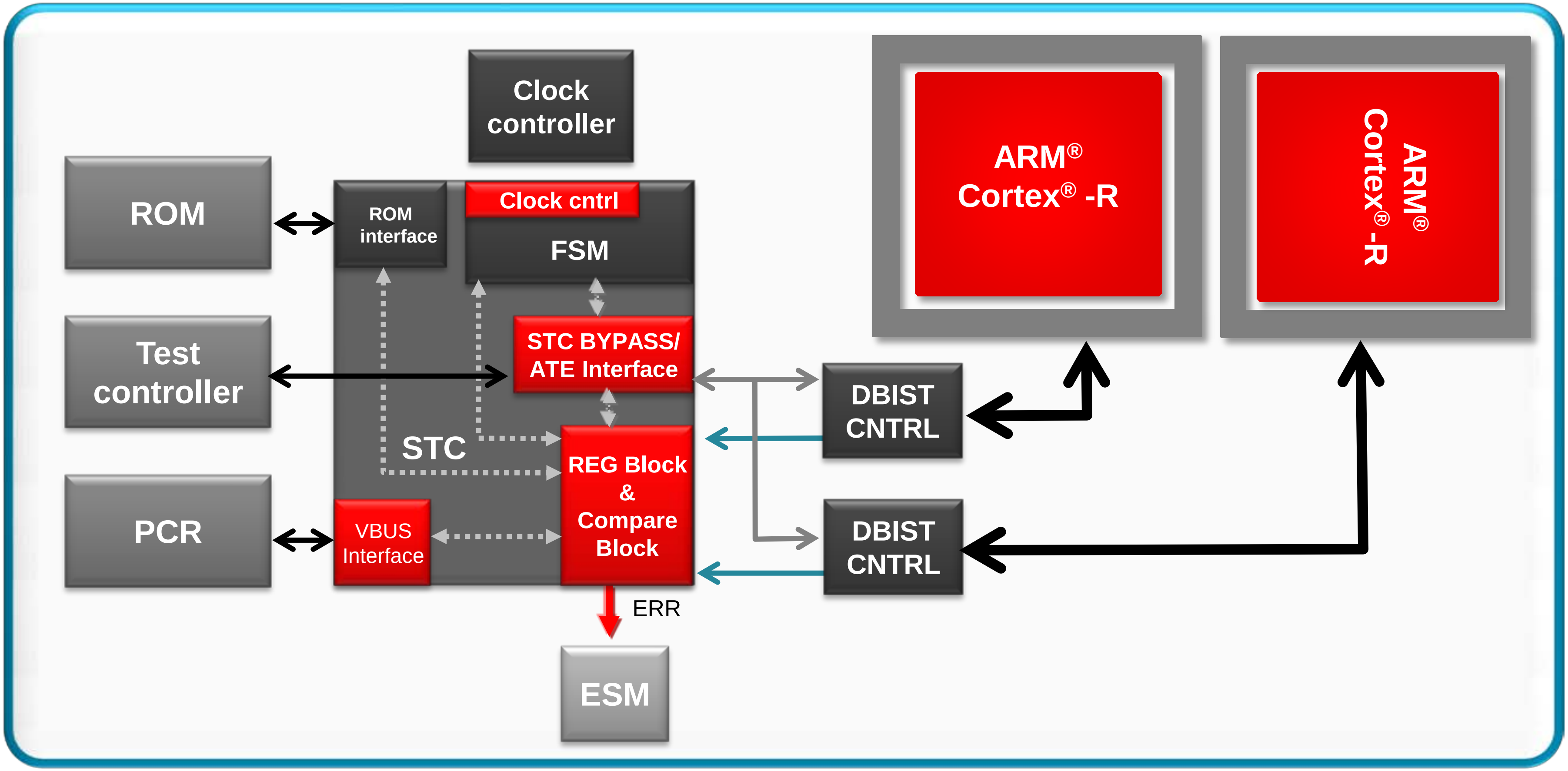
Real-time / Determinism

- ❑ Tightly Coupled Memory (TCM)
- ❑ Fast interrupt response
- ❑ Deterministic interrupt response

*Cortex R5 based products



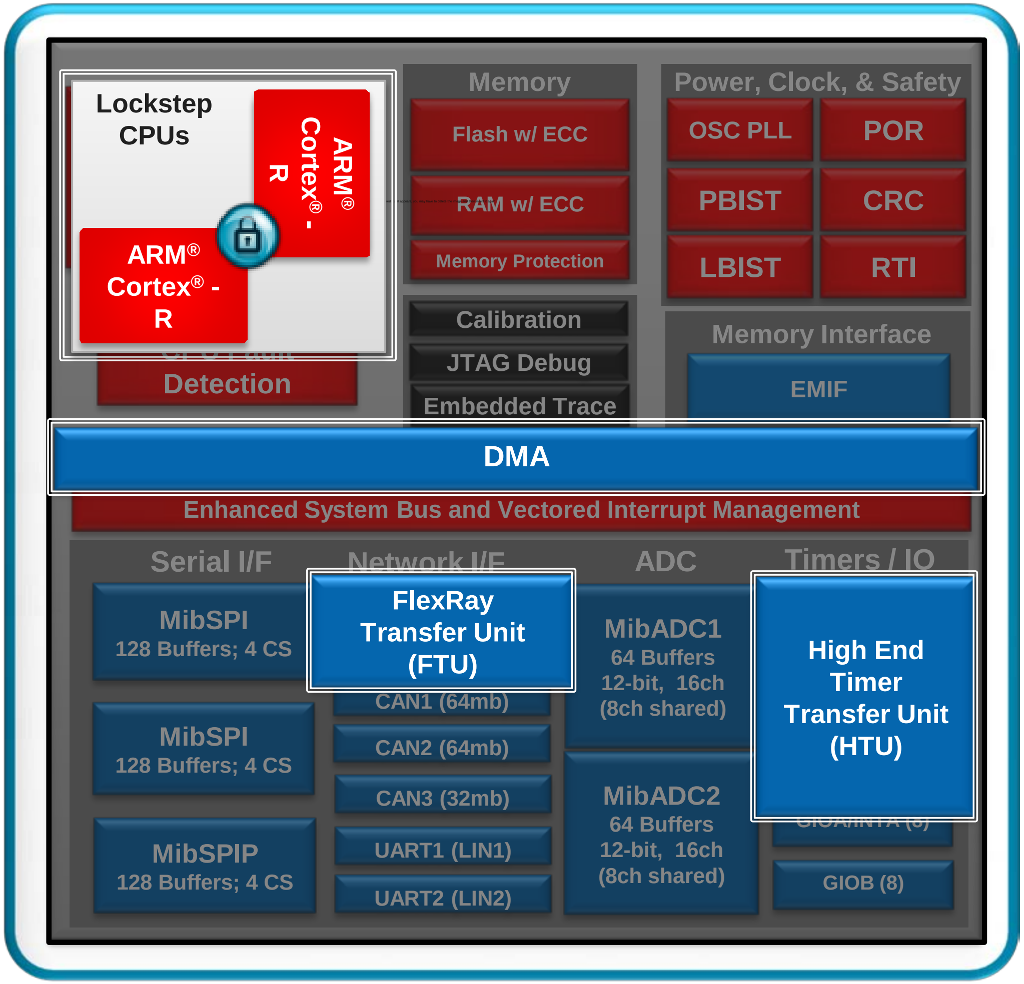
CPU Self Test Controller (STC/LBIST)



- Provides High Diagnostic Coverage
- Significantly Lowers S/W and Runtime Overhead
- No SW BIST (Built In Self Test) Code overhead in Flash
- Simple to configure and start BIST via register

Memory Protection Unit (MPU)

- A Dedicated Memory Protection Unit (MPU) is implemented for select bus masters



Bus masters include the CPU, DMA, HTU and the FTU

A memory region is defined which allows read and write access for the bus master

Access outside the defined region can be any of the mode

Read Only: Read access allowed for the memory accesses outside the region. Write accesses are blocked

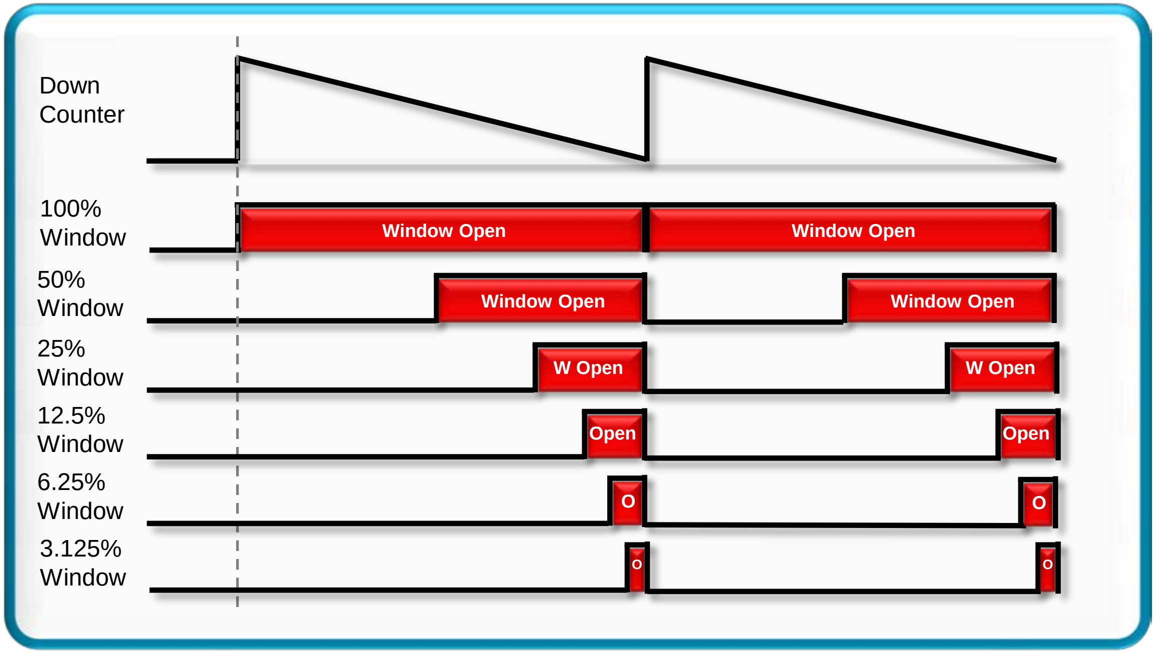
No Access: Read and write access is blocked.

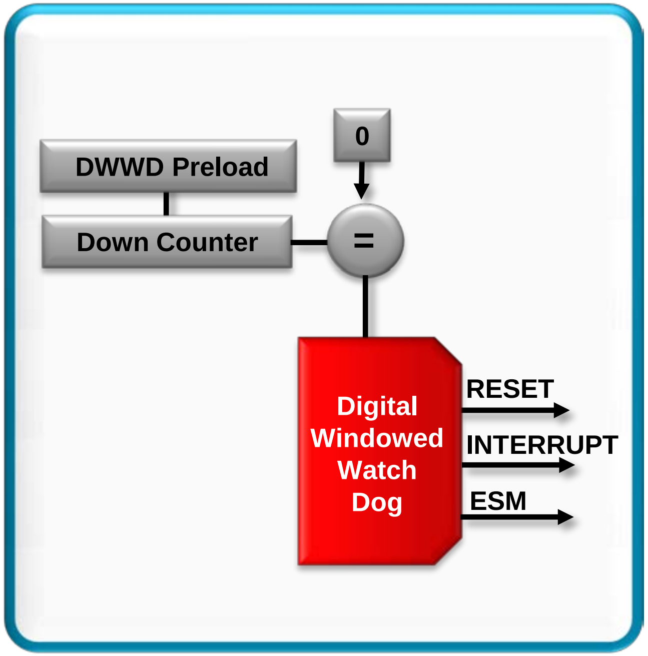
In the event of a detected memory protection violation an error is indicated

Note: This is a simplified view. The programmer's model differs between IP. CPU IP will have significantly more options to control access via the MPU.

Digital Windowed Watch Dog (DWWD)

- The DWWD module will reset the MCU or generate a non maskable interrupt to the CPU if the application fails to service the watchdog within the appropriate time window.
  - Safety diagnostic that can detect a runaway CPU
  - Includes a 25-bit down counter
  - Alerts the Error Signaling Module when a CPU interrupt is generated
  - Supports multiple service windows: 100%, 50%, 25%, 12.5%, 3.125%
  - Servicing requires a specific two part key sequence
  - Once enabled can only be disabled by a system or power on reset





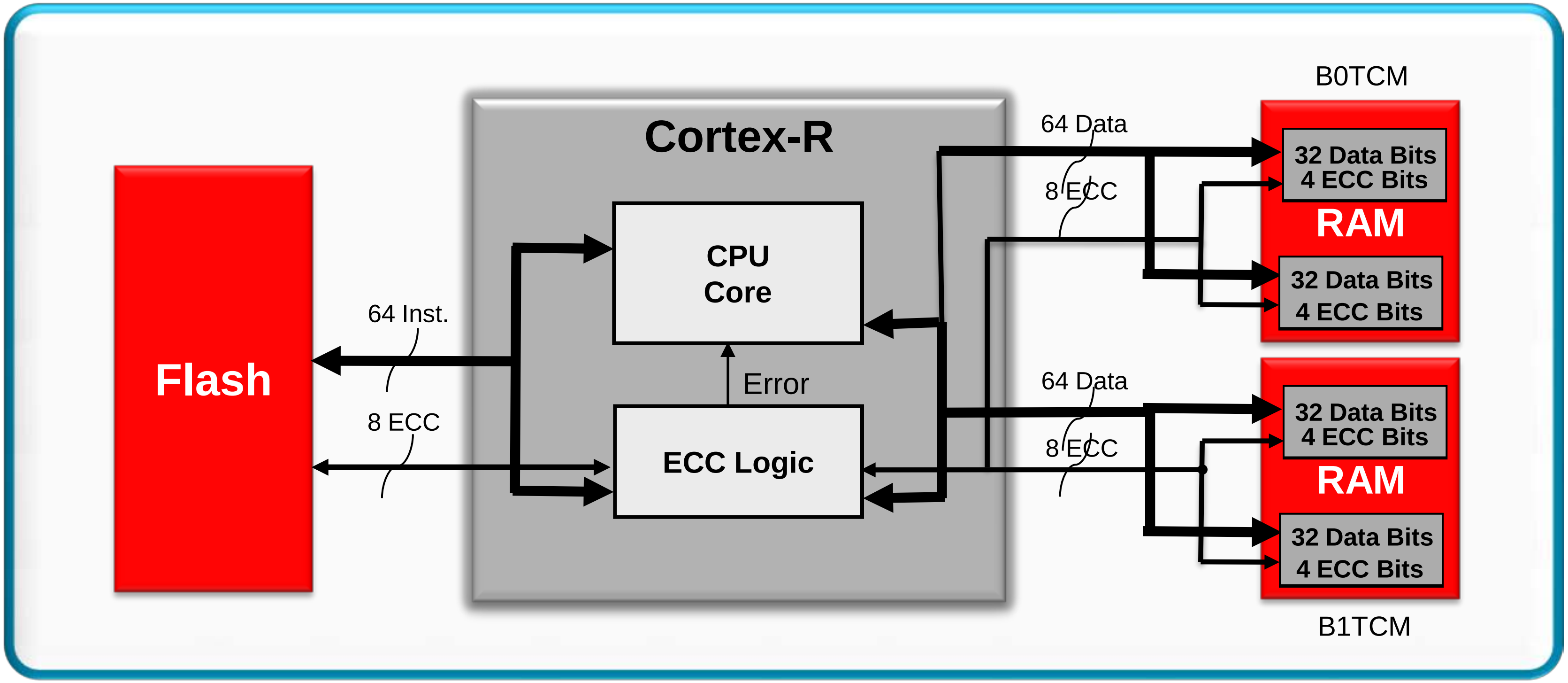
IEC61508 HW Metrics Calculation Select Safety Features - Flash

From Safety Manual				
Device Partition	**Unique identifier**	**Safety Feature or Diagnostic**	**Feature Reccomendation**	**Diagnostic Used in Application?**
Primary Flash and Level 1 (L1) Interconnect	FLA1	Flash Data ECC	++	1
Primary Flash and Level 1 (L1) Interconnect	FLA2	Hard error cache and livelock	M	1
Primary Flash and Level 1 (L1) Interconnect	FLA3	Flash wrapper address ECC	++	1
Primary Flash and Level 1 (L1) Interconnect	FLA4	Address parity	++	1
Primary Flash and Level 1 (L1) Interconnect	FLA5A	Boot time hardware CRC check of flash memory contents	++	1
Primary Flash and Level 1 (L1) Interconnect	FLA5B	Periodic hardware CRC check of flash memory contents	+	1
Primary Flash and Level 1 (L1) Interconnect	FLA6	Bit multiplexing in flash array	M	1
Primary Flash and Level 1 (L1) Interconnect	FLA7	Flash sector protection	++	1
Primary Flash and Level 1 (L1) Interconnect	FLA8	Periodic SW readback of static configuration registers	+	1
Primary Flash and Level 1 (L1) Interconnect	FLA9	SW readback of written configuration	++	1

- Safety Mechanisms associated with Flash are selected.
  - '1' means the safety mechanism is assumed in the HW metrics calculation
  - '0' means not assumed

Based on RM42x/LS04x/LS03x v0.8 FMEDA worksheet

Flash / RAM ECC Protection



ECC evaluated in the Cortex-R CPU

- Single Bit Error Correction and Double Bit Error Detection (SECDED)
- ECC evaluated in parallel to processing data/instructions
- Minimized latency and typically no performance impact
- Protects Busses from CPU to Flash and RAM

– Address / Control parity from CPU -> Memory

– Diagnostic in Flash / SRAM wrappers

IEC61508 HW Metrics Calculation Select Safety Features - SRAM

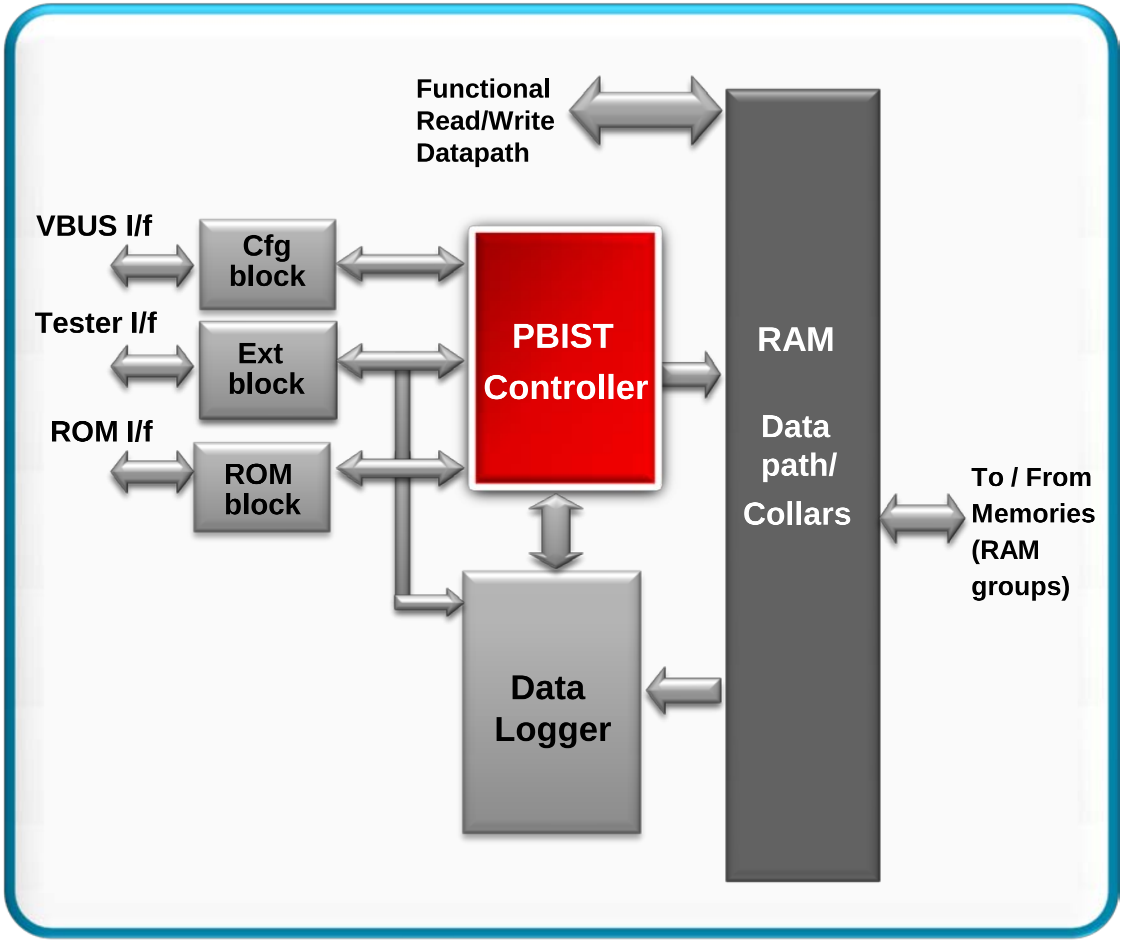
From Safety Manual				
Device Partition	**Unique identifier**	**Safety Feature or Diagnostic**	**Feature Reccomendation**	**Diagnostic Used in Application?**
SRAM and Level 1 (L1) Interconnect	RAM1	Data ECC	++	1
SRAM and Level 1 (L1) Interconnect	RAM2	Hard error cache and livelock	M	1
SRAM and Level 1 (L1) Interconnect	RAM3	Correctable ECC profiling	+	1
SRAM and Level 1 (L1) Interconnect	RAM4	Address and control parity	++	1
SRAM and Level 1 (L1) Interconnect	RAM5	Redundant address decode	++	1
SRAM and Level 1 (L1) Interconnect	RAM6	Data/ECC storage in multiple physical banks	M	1
SRAM and Level 1 (L1) Interconnect	RAM7A	Boot time PBIST check of RAM	++	1
SRAM and Level 1 (L1) Interconnect	RAM7B	Periodic PBIST check of RAM	O	0
SRAM and Level 1 (L1) Interconnect	RAM8	Bit multiplexing in SRAM array	M	1
SRAM and Level 1 (L1) Interconnect	RAM9	Periodic hardware CRC check of SRAM contents	O	0
SRAM and Level 1 (L1) Interconnect	RAM10	Periodic SW readback of static configuration registers	+	1
SRAM and Level 1 (L1) Interconnect	RAM11	SW readback of written configuration	++	1
SRAM and Level 1 (L1) Interconnect	RAM12	SW driven RAM red.decoder and ECC test	++	1

- Safety Mechanisms associated with SRAM are selected.
  - ‘1’ means the safety mechanism is assumed in the HW metrics calculation
  - ‘0’ means not assumed

Based on RM42x/LS04x/LS03x v0.8 FMEDA worksheet

Programmable Memory BIST (PBIST)

- All on-chip RAMS can be tested
- Simple register setup and configuration
- Typically run at startup, but can be executed during the application
- Multiple Memory Test Algorithms
- Detects multiple failure modes



- Provides a mechanism to determine if runtime faults were caused by hard or soft error. This capability can be used to improve availability through inline recovery from soft error.

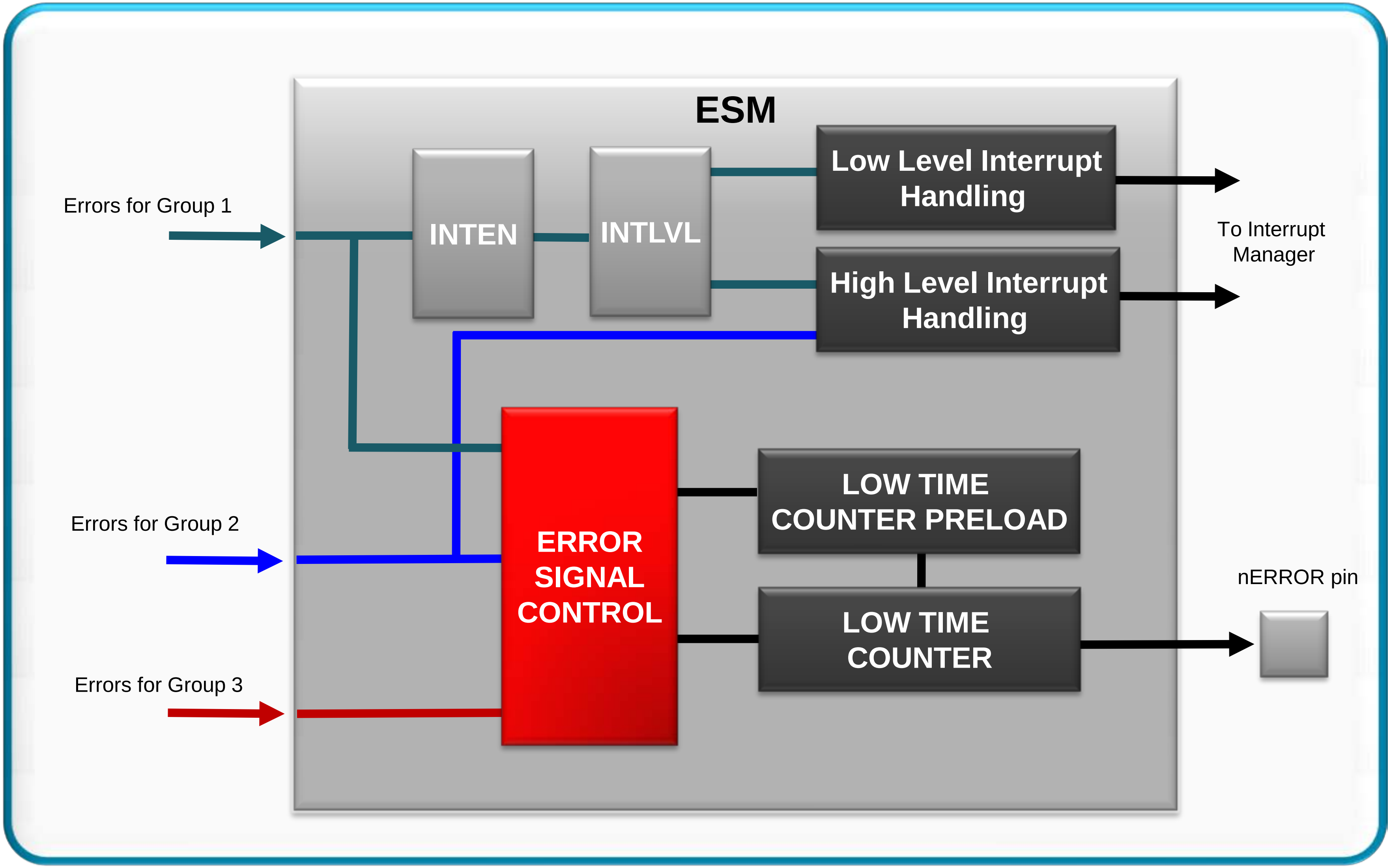
IEC61508 HW Metrics Calculation
Select Safety Features - ESM

From Safety Manual					
Device Partition	**Unique identifier**	**Safety Feature or Diagnostic**	**Feature Reccomendation**		**Diagnostic Used in Application?**
Error Signaling Module (ESM)	ESM1	Periodic SW readback of static configuration registers	+		1
Error Signaling Module (ESM)	ESM2A	Boot time SW test of error path reporting	++		1
Error Signaling Module (ESM)	ESM2B	Periodic SW test of error path reporting	+		1
Error Signaling Module (ESM)	ESM3	Use of status shadow registers	++		1
Error Signaling Module (ESM)	ESM4	SW readback of written configuration	++		1

- Safety Mechanisms associated with ESM are selected.
  - ‘1’ means the safety mechanism is assumed in the HW metrics calculation
  - ‘0’ means not assumed

Based on RM42x/LS04x/LS03x v0.8 FMEDA worksheet

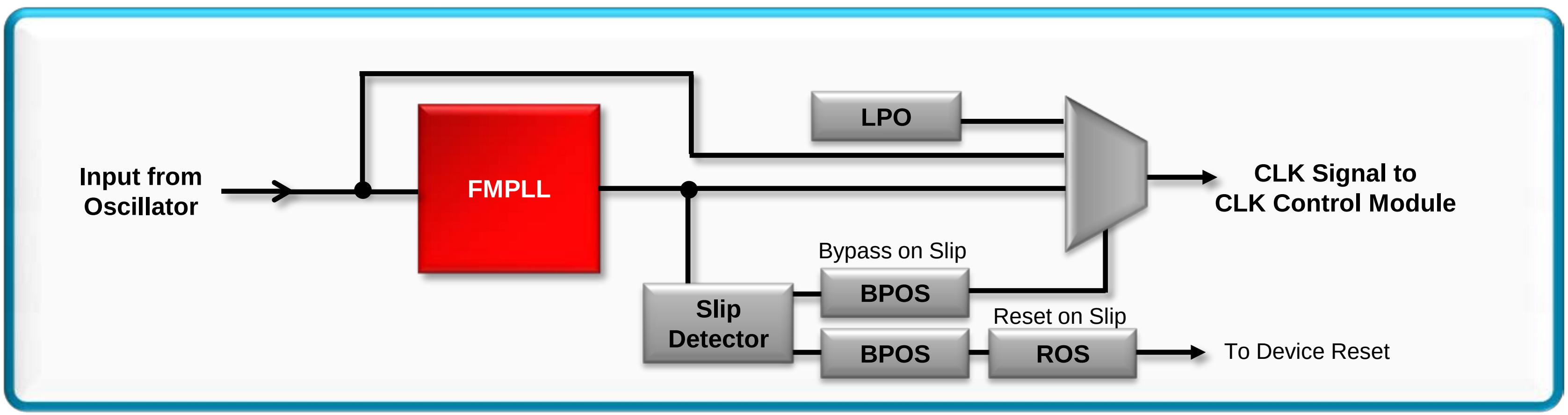
Error Signaling Module (ESM)



Clock Monitoring

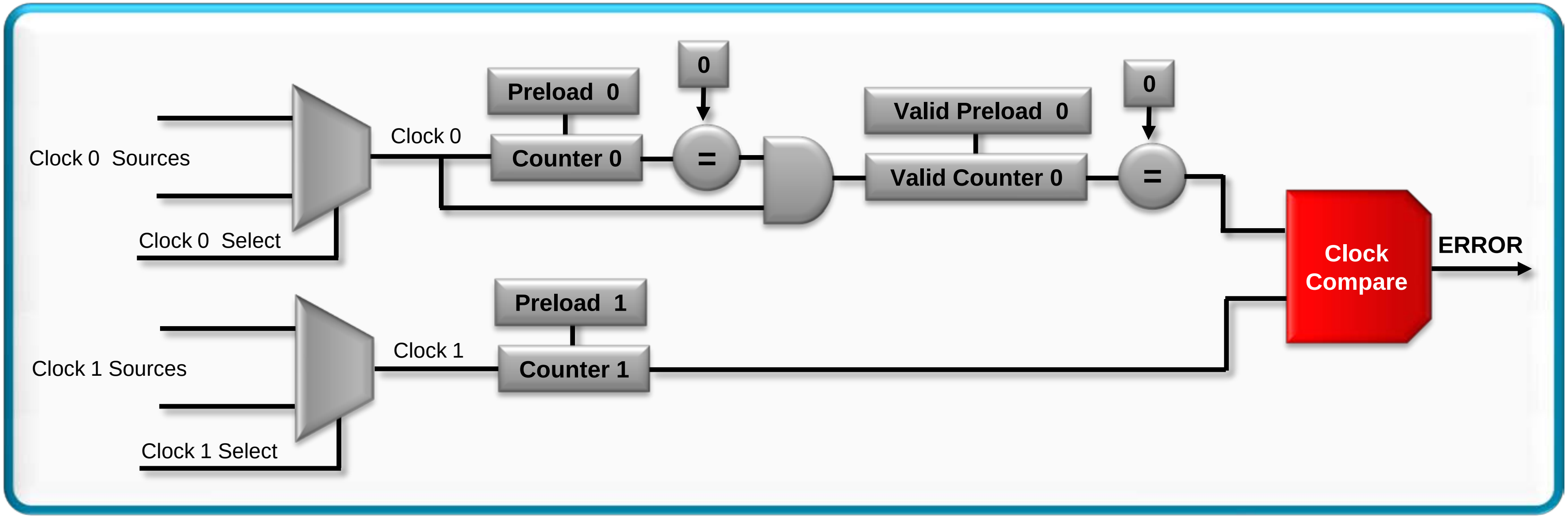
- External clock prescaler (ECLK)
  - Allows external monitoring of CPU clock frequency
  - Configurable pin (GIO or ECLK)
- Oscillator monitor
  - Detects failure if oscillator frequency exceeds defined min/max thresholds*
  - Selectable hardware response on oscillator fail
    - Reset device
    - Switch to internal 'low power oscillator' (LPO) clock source
- FMPLL slip detector
  - Indicates PLL slip if phase lock is lost
  - Selectable hardware response on PLL slip
    - Reset device
    - Switch to internal 'low power oscillator' (LPO) clock source
    - Switch to external oscillator clock source

* Refer to device data sheet



Dual Clock Comparator (DCC)

- The DCC module is used to measure the frequency of a clock signal using a second clock signal as a reference.
  - Allows application to ensure that a fixed frequency ratio is maintained between two clock signals
  - Supports the definition of a programmable tolerance window in terms of number of reference clock cycles
  - Supports continuous monitoring without requiring application intervention
  - Alternatively can be used in a single-sequence mode for spot measurements
  - Flexible clock source selection for Counter 0 and Counter 1 resulting in several specific use cases



IEC61508 HW Metrics Calculation Select Safety Features - CAN

From Safety Manual				
Device Partition	**Unique identifier**	**Safety Feature or Diagnostic**	**Feature Reccomendation**	**Diagnostic Used in Application?**
Controller Area Network (DCAN)	CAN1A	Boot time SW test of function using I/O loopback	++	1
Controller Area Network (DCAN)	CAN1B	Periodic SW test of function using I/O loopback	O	0
Controller Area Network (DCAN)	CAN2	Information redundancy techniques including end to end safing	++	1
Controller Area Network (DCAN)	CAN3	DCAN SRAM Data Parity	++	1
Controller Area Network (DCAN)	CAN4A	Boot time PBIST check of DCAN RAM	++	1
Controller Area Network (DCAN)	CAN4B	Periodic PBIST check of DCAN RAM	O	0
Controller Area Network (DCAN)	CAN5	Bit multiplexing in DCAN RAM array	M	1
Controller Area Network (DCAN)	CAN6	Periodic hardware CRC check of DCAN SRAM contents	O	0
Controller Area Network (DCAN)	CAN7	Periodic SW readback of static configuration registers	+	1
Controller Area Network (DCAN)	CAN8	Software readback of written configuration	++	1

- Safety Mechanisms associated with CAN are selected.
  - ‘1’ means the safety mechanism is assumed in the HW metrics calculation
  - ‘0’ means not assumed

Based on RM42x/LS04x/LS03x v0.8 FMEDA worksheet

IEC61508 HW Metrics Calculation
Select Safety Features – Power Supply

Device Partition	Unique identifier	Safety Feature or Diagnostic	Feature Reccomendation	Diagnostic Used in Application?
Power Supply	PWR1	Voltage monitor (VMON)	M	1
Power Supply	PWR2	External voltage supervisor	++	1

- Safety Mechanisms associated with Power Supply are selected.
  - ‘1’ means the safety mechanism is assumed in the HW metrics calculation
  - ‘0’ means not assumed

Based on RM42x/LS04x/LS03x v0.8 FMEDA worksheet

IEC61508 HW Metrics Calculation Select Safety Features - Package

- High diagnostic coverage is assumed for the package via detection of failure with existing diagnostics supplemented by application level diagnostics.
  - Examples:
    - CAN - CAN2 Information Redundancy Technique and CAN1A Boot-time I/O loop back SW test
    - MIBSPI - MSP2 Information Redundancy Technique and MSP1A Boot-time I/O loop back SW test

Extracted from Safety Manual of RM42x spnu553

IEC61508 HW Metrics Calculation
Select Safety Features – IO Loop Back

- Hercules MCU I/O supports loop back for self-test. Below are examples:

Figure 24-16. CAN Core in Loop Back Mode

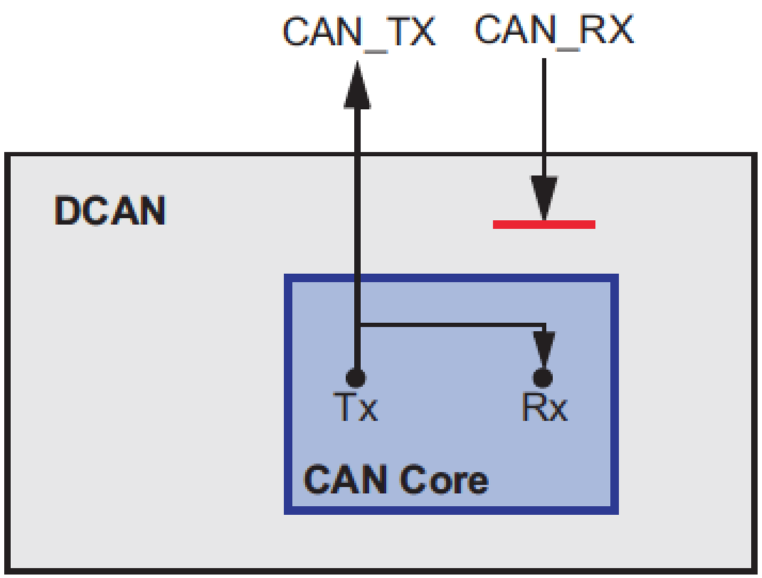
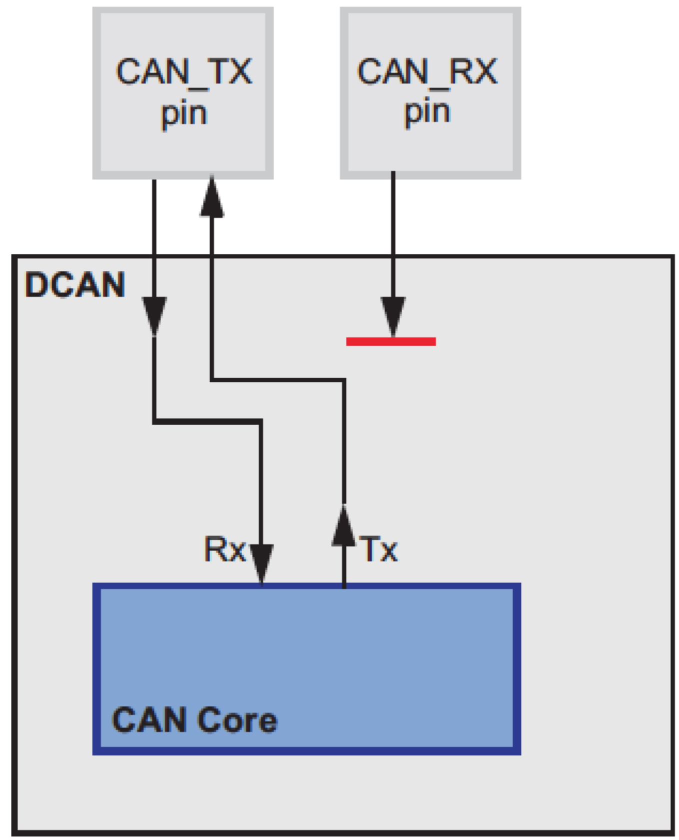


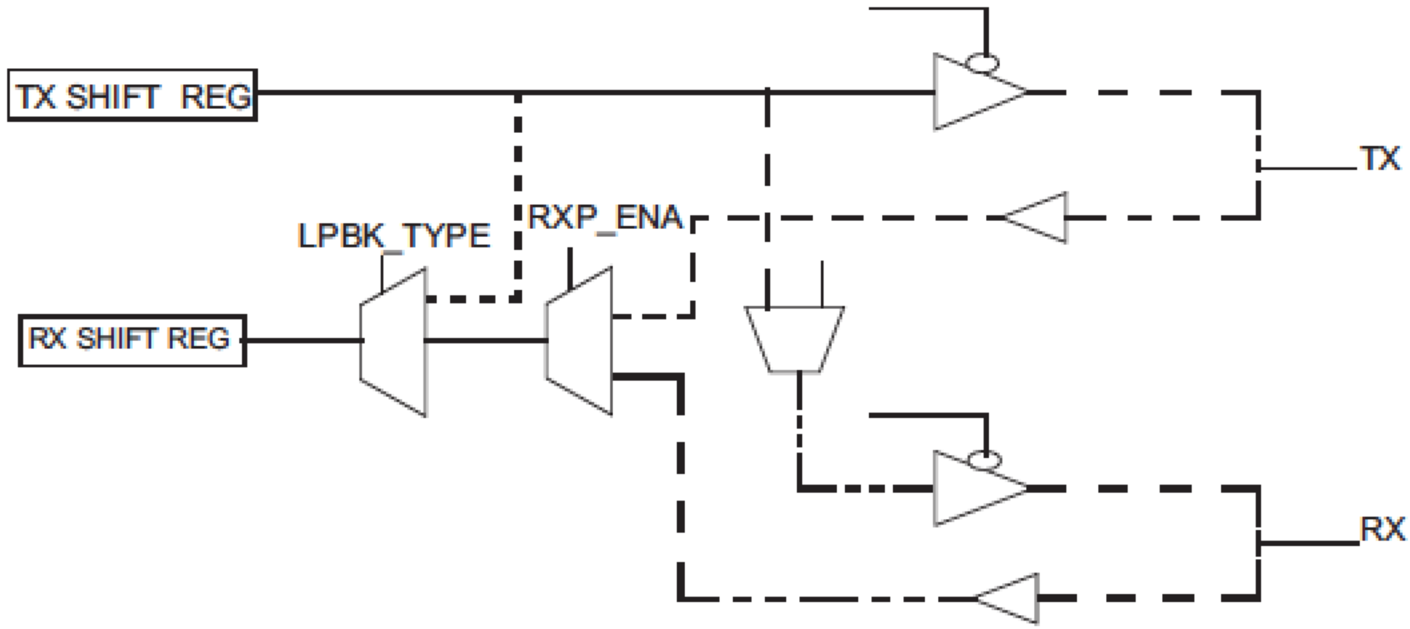
Figure 24-17. CAN Core In External Loop Back Mode



Examples are extracted from TMS570LS31x/21x Technical Reference Manual SPNU499a

IEC61508 HW Metrics Calculation
Select Safety Features – IO Loop Back

Figure 25-22. I/O Paths during I/O Loopback Modes



- – – Checks the analog loopback path through the receive buffer
- —— Checks the analog loopback path through the transmit buffer
- ▪▪▪▪ Digital loopback path

1 This diagram is intended to illustrate loopback paths and therefore may omit some normal-mode paths.

Examples are extracted from TMS570LS31x/21x Technical Reference Manual SPNU499a

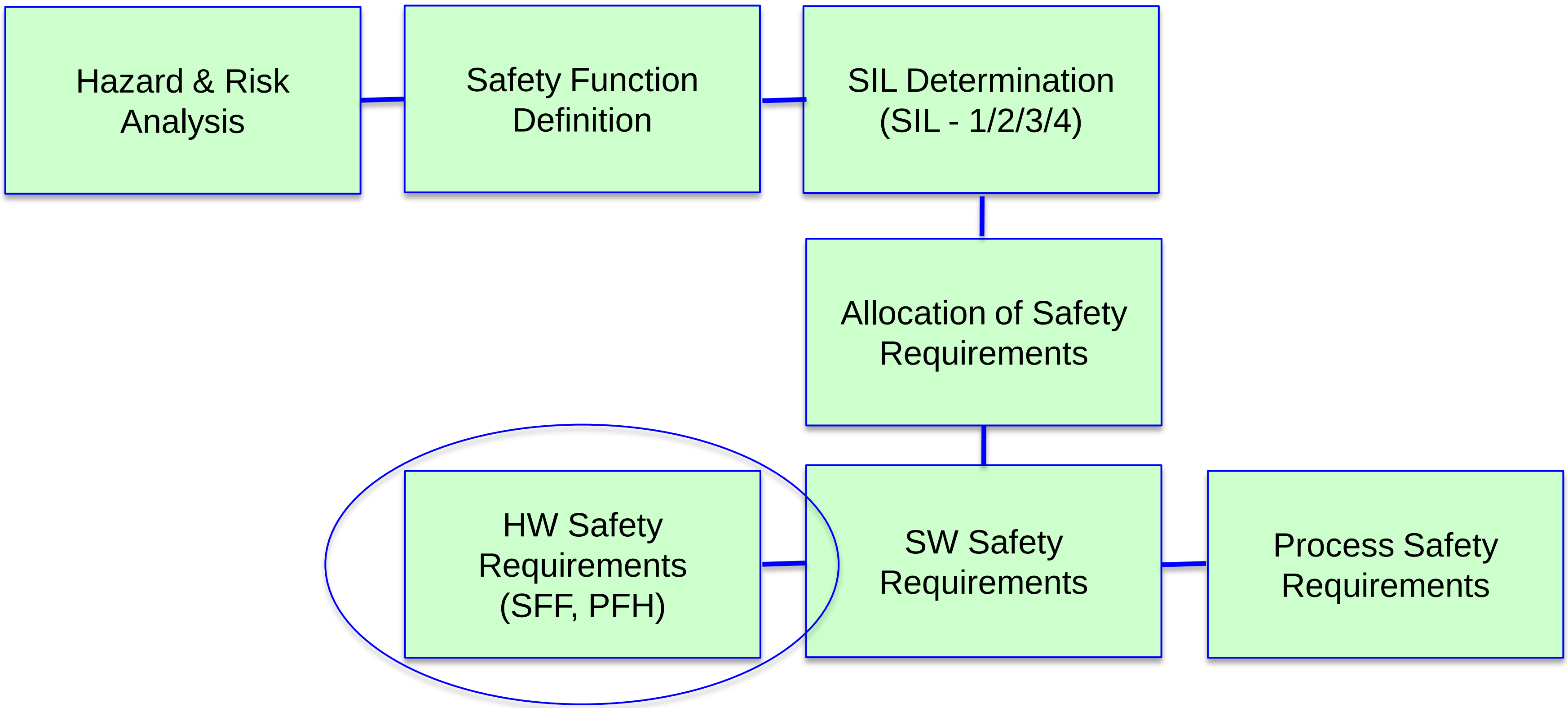
Agenda

- Overview of Hercules^{TM} MCU and SafeTI^{TM} Design package
- Hercules^{TM} MCU Functional Safety How-To Workshop
  - Safety Functions, Safety Goals, Safe State, SIL, Failure rate
  - Safety Critical Elements identification and Diagnostic Requirements
  - Safety Manual and Diagnostics Selection
  - Mission Profile and Failure Rate Estimation
  - SafeTI^{TM} Diagnostic Library
  - SafeTI^{TM}I Diagnostic Library Compliance Support Package (CSP) certification support
  - Fault Injection with HITEX kit
- Summary

Estimate SFF / PFH per Safety Function

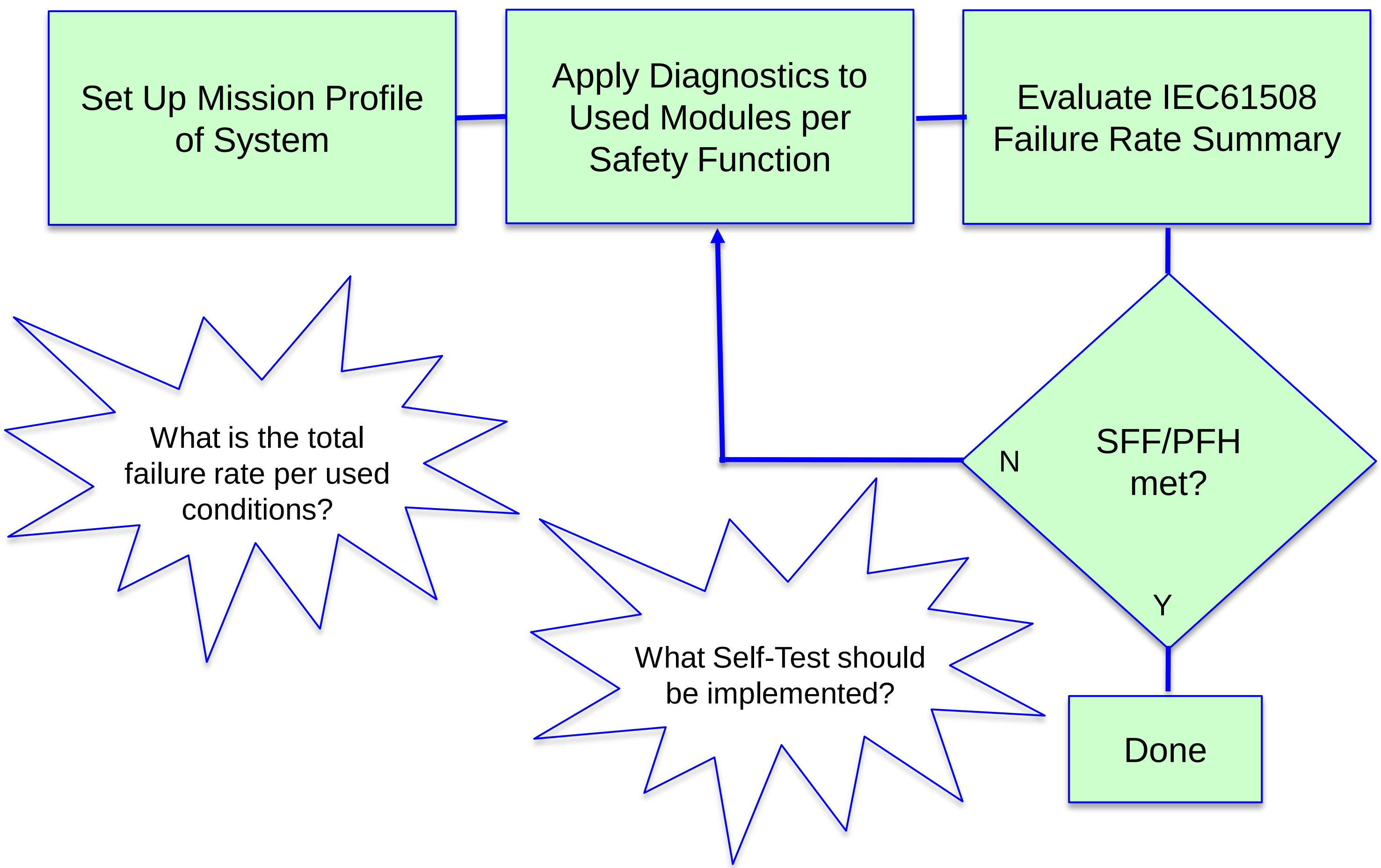
Now we have a safety function and SIL requirement,

→ How to estimate the SFF / PFH to determine if SIL requirement can be met?

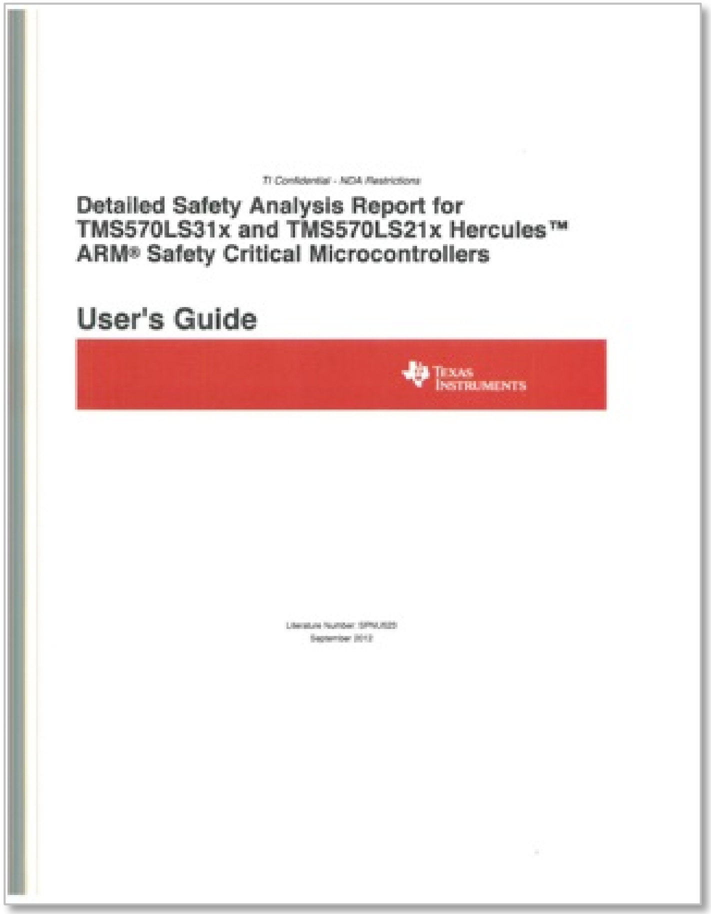


Estimate MCU SFF / PFH per Safety Function

Use Hercules MCU Detailed Safety Analysis Report & FMEDA worksheet



Detailed Safety Analysis Report & FMEDA worksheet


TI Confidential - NDA Restrictions

Detailed Safety Analysis Report for TMS570LS31x and TMS570LS21x Hercules™ ARM® Safety Critical Microcontrollers

User's Guide

Available under NDA

Detailed Safety Analysis Report

- Assumptions of use applied in calculation of safety metrics
- Summary of IEC 61508 or ISO 26262 standard safety metrics at the MCU component level
- A fault model used to estimate device failure rates and an example of customizing this model for use with the example application.
- FMEDA with details to the sub-module level of the MCU, that enables calculation of safety metrics based on customized application of diagnostics

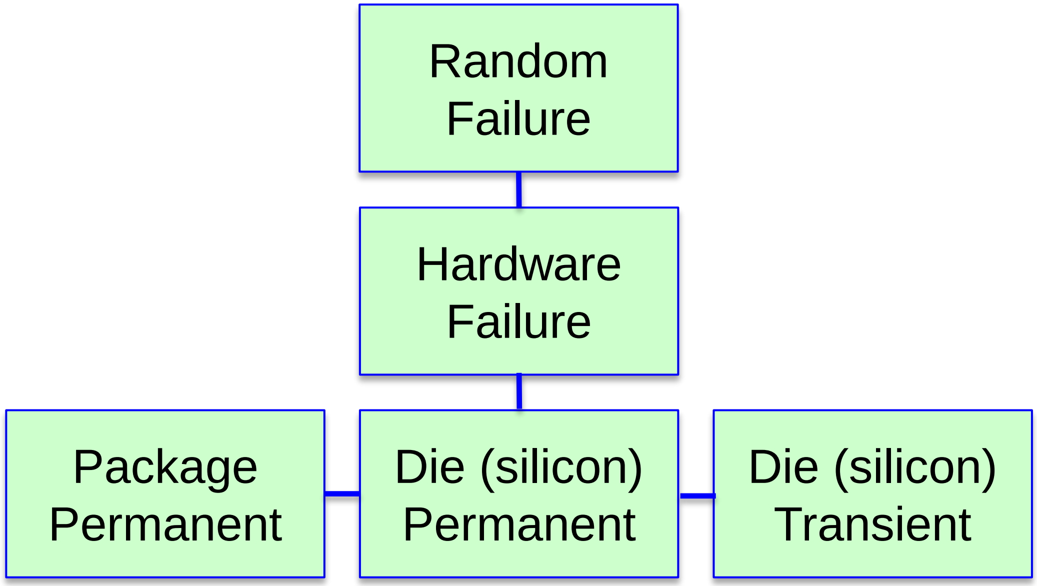
4.2 Summary of IEC 61508 Safety Metrics at Device Level (BGA Package)

Table 3 provides estimates of FIT rates and calculated safety metrics per IEC 61508-2:2010 using previously noted assumptions for the device in BGA package.

Total FIT (Raw FIT)	λ
Safety Related FIT	λ_{SR}
Probability of Hardware Failures (in FIT)	PFH
Safe Failure Fraction	SFF

Total faults	λ
Total non safety related faults	λ_{nSR}
Total safe faults	λ_S
Total dangerous faults	λ_D
Total dangerous detected faults	λ_{DD}
Total dangerous undetected faults	λ_{DU}

IEC61508 HW Metrics Calculation
Failure Rate



Multiple Ways for Random failure rate estimation:

- MIL-HDBK-217F, "Military Handbook - Reliability Prediction of Electronic Equipment"
- Siemens Norm SN29500:2010, "Failure Rates of Components"
- Supplier reliability data from similar products already in production and deployed under similar operating conditions
- IEC/TR 62380:2004, "Reliability Data Handbook - Universal Model for Reliability Prediction of Electronics, PCBs, and Equipment"

- TI has selected to use IEC/TR 62380 because it is more aligned to semiconductor physics models
- Failure rate is measured in FIT where 1 FIT is 1 fail in 10^9 operating hours

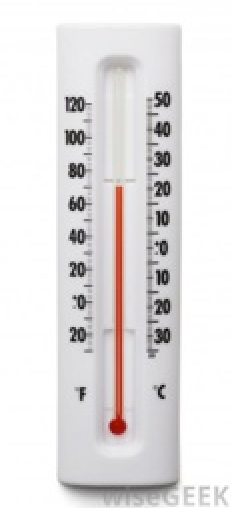
IEC61508 HW Metrics Calculation
Failure Rate / Mission Profiles

Random Failure

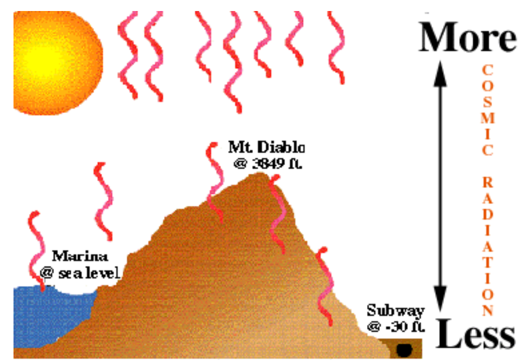
Hardware Failure

Package Permanent | Die (silicon) Permanent | Die (silicon) Transient









IEC/TR 62380 Mission Profiles Examples

Source: IEC/TR 62380 Reliability Handbook

Table 11 – Mission profiles for automotive

Mission profile phases	Temp. 1		Temp. 2		Temp. 3		Ratios on/off		2 night starts		4 day light starts		Non used vehicle	
Application types	$(t_{ac})_1$ °C	τ_1	$(t_{ac})_2$ °C	τ_2	$(t_{ac})_3$ °C	τ_3	τ_{on}	τ_{off}	n_1 cycles/year	ΔT_1 °C/cycle	n_2 cycles/year	ΔT_2 °C/cycle	n_3 cycles/year	ΔT_3 °C/cycle
Motor control	32	0.020	60	0.015	85	0.023	0.058	0.942	670	$\frac{\Delta Tj}{3}+55$	1340	$\frac{\Delta Tj}{3}+45$	30	10
Passenger compartment	27	0.006	30	0.046	85	0.006	0.058	0.942	670	$\frac{\Delta Tj}{3}+30$	1340	$\frac{\Delta Tj}{3}+20$	30	10

Table 9 – Mission profiles for Telecom

Environment types	Equipment types	$(t_{ae})_i$ °C	$(t_{ac})_i$ °C	τ_1	τ_{on}	τ_{off}	n_1 cycles/year	ΔT_1 °C/cycle
Ground; benign: (G_B)	switching	20	30	1	1	0	365	0
Ground; benign: (G_B)	Transmitting	20	40	1	1	0	365	0
Ground; fixed: (G_F)	Transmitting and access	11	31	1	1	0	365	8

IEC61508 HW Metrics Calculation Automotive Motor Control Mission Profiles

- Automotive Mission Profile in IEC/TR 62380 (FMEDA worksheet default):
  - 10 years service with 3 phases per day – night, day, not used
    - 2 night trips per day, 4 day trips per day, 30 days shut down
  - 3 temperature phases
    - Engine cold, Engine warm, Engine hot
  - On/Off ratio: 0.058 / 0.942

Customer input for failure rate estimation

Package Used	TI PBGA
Customer input for transient fault estimation Application specific Flux Factor coeff. based on Jedec JESD89A	1
Maximum power dissipation Application specific power dissipation in Watts (1.04W is based on maximum datasheet value)	1.04
Assumed Lifetime in years	10
Confidence Level Desired confidence level of FIT rates	70%

Automotive Mission Profile:
Total raw die permanent FIT: 9.48

Based on RM48x v1.0 FMEDA worksheet

Operational Profile from IEC/TR 62380:2004

	Temp1		Temp2		Temp3		Ratios on/off		2 night starts		4 day light starts		Non used vehicle	
	$(t_{ac})_1$ °C	$\tau 1$	$(t_{ac})_2$ °C	$\tau 2$	$(t_{ac})_3$ °C	$\tau 3$	T_{on}	T_{off}	n_1	ΔT_1 °C	n_2	ΔT_2	n_3	ΔT_3
Profile	32	0.02	60	0.015	85	0.023	0.058	0.942	670	ΔTj/3+55	1340	ΔTj/3+45	30	10

IEC61508 HW Metrics Calculation Elevator Mission Profiles

- Assumed Elevator/Escalator mission profile:
  - 10 years service, 365 days per year, 18 hours on and 6 hours off per day
  - T_{ae} outside ambient temp = 25c (indoor ambient temp)
  - T_{ac} PCB temp = 60c
  - $T_{on} = 0.75$, $T_{off} = 0.25$
  - N = 1 x 365 cycles
  - ΔT_j (chip junction temp increased vs T_{ac}) = 30c (assumed worst case)
  - $\Delta T = \Delta T_j/3 + (60\text{-}25)c = 55c$

Customer input for failure rate estimation

Package Used — TI PBGA

Customer input for transient fault estimation
Application specific Flux Factor coeff. based on Jedec JESD89A — 1

Maximum power dissipation
Application specific power dissipation in Watts
(1.04W is based on maximum datasheet value) — 1.04

Assumed Lifetime
in years — 10

Confidence Level
Desired confidence level of FIT rates — 70%

Elevator Mission Profile:
Total raw permanent FIT: 103.37

Based on RM48x v1.0 FMEDA worksheet

Operational Profile from IEC/TR 62380:2004

	Temp1		Temp2		Temp3		Ratios on/off		Daily on/off	
	$(t_{ac})_1$ °C	$\tau 1$	$(t_{ac})_2$ °C	$\tau 2$	$(t_{ac})_3$ °C	$\tau 3$	T_{on}	T_{off}	n_1	ΔT_1 °C
Profile	32	0	60	0.75	85	0	0.75	0.25	365	0

TEXAS INSTRUMENTS

IEC61508 HW Metrics Calculation Industrial Mission Profiles

- Assumed Industrial mission profile:
  - 10 years service, 365 days per year, 24 hours per day
  - T_{ae} outside ambient temp = 70c (ambient temp)
  - T_{ac} PCB temp = 90.5c (assumption)
  - T_{on} = 1, T_{off} = 0
  - n = 1 cycles
  - ΔT_j (chip junction temp increased vs T_{ac}) = 30c (assumed worst case)
  - $\Delta T = \Delta T_j/3 + (90.5\text{-}70)c = 30.5c$

Customer input for failure rate estimation

Package Used	TI PBGA
Customer input for transient fault estimation Application specific Flux Factor coeff. based on Jedec JESD89A	1
Maximum power dissipation Application specific power dissipation in Watts (1.04W is based on maximum datasheet value)	1.04
Assumed Lifetime in years	10
Confidence Level Desired confidence level of FIT rates	70%

Industrial Mission Profile:
Total raw permanent FIT: 330.16

Based on RM48x v1.0 FMEDA worksheet

Operational Profile from IEC/TR 62380:2004 Echo use conditions

	Temp1		Temp2		Temp3		Ratios on/off		Number of On/off per year	
	$(t_{ac})_1$ °C	$\tau 1$	$(t_{ac})_2$ °C	$\tau 2$	$(t_{ac})_3$ °C	$\tau 3$	T_{on}	T_{off}	n_1	ΔT_1 °C
Profile	92.5	1	0	0	0	0	1	0	1	0

Failure Rate Definitions

- Failure rate is represented with the Greek character lambda, λ, and can be broken into many categories.
  - λ_S: rate of safe failures which do not affect safety function
    - λ_{SD} : safe, detected failure rate
    - λ_{SU} : safe, undetected failure rate
  - λ_D: rate of dangerous failures which compromise the safety function
    - λ_{DD} : dangerous, detected failure rate
    - λ_{DU} : dangerous, undetected failure rate

- Note: a failure which results in the system changing mode of operation to a safe state is by definition a safe failure.

- Failure rate is often expressed in FITs. One FIT (Failure In Time) = 1 failure per billion hours of operation (1x 10^{-9} failures/hour)

IEC61508 HW Metrics vs Mission Profiles

IEC61508 HW metrics with Automotive Mission Profile (70% confidence level):

Numbers are normalized to Die Permanent Total RAW FIT

	Die		Package	Overall
	Permanent	Transient	Permanent	Sum
Total FIT (Raw FIT)	10.00	764.40	69.89	844.30
Safety related FIT	9.97	734.58	68.95	813.49
Probability of Hardware Failures - PFH (in FIT)	0.06	0.82	0.13	1.01
Safe Failure Fraction - SFF	99.36%	99.89%	99.82%	99.88%

IEC61508 HW metrics with Elevator Mission Profile (70% confidence level):

Numbers are normalized to Automotive Mission Profile Die Permanent Total RAW FIT

	Die		Package	Overall
	Permanent	Transient	Permanent	Sum
Total FIT (Raw FIT)	108.99	764.44	13.12	886.55
Safety related FIT	108.67	734.61	12.95	856.24
Probability of Hardware Failures - PFH (in FIT)	0.69	0.82	0.06	1.57
Safe Failure Fraction - SFF	99.36%	99.89%	99.54%	99.82%

IEC61508 HW metrics with Industrial Mission Profile (70% confidence level):

Numbers are normalized to Automotive Mission Profile Die Permanent Total RAW FIT

	Die		Package	Overall
	Permanent	Transient	Permanent	Sum
Total FIT (Raw FIT)	348.11	764.53	2.69	1115.33
Safety related FIT	347.09	734.71	2.69	1084.48
Probability of Hardware Failures - PFH (in FIT)	2.20	0.84	0.12	3.16
Safe Failure Fraction - SFF	99.36%	99.89%	95.45%	99.71%

- Higher raw permanent FIT rate because of much longer ‘on’ time
- No significant difference of Safe Failure Fraction (SFF)
- Probability of Hardware Failure (PFH) increases in proportion to raw rate rate increase.

Based on RM48x v1.0 FMEDA worksheet

IEC61508 HW Metrics Calculation Impact of Confidence Level

Confidence level	70%				
Permanent FIT	6.20E-10				
Transient FIT	6.80E-10	Elevator mission profile			
Package FIT	6.00E-11				
Overall FIT	1.36E-09				
Number of units in field	1000000				
Number of device hours per day	18				
Device operating year	1	5	10	15	20
Total number of device operating year	1.00E+06	5.00E+06	1.00E+07	1.50E+07	2.00E+07
Total number of device operating hours	6.57E+09	3.29E+10	6.57E+10	9.86E+10	1.31E+11
Estimated number of failures due to Permanent fault	4.1	20.4	40.7	61.1	81.5
Estimated number of failures due to Transient fault	4.5	22.3	44.7	67.0	89.4
Estimated number of failures due to Package fault	0.4	2.0	3.9	5.9	7.9
Estimated number of failures due to Overall fault	8.9	44.7	89.4	134.0	178.7

Confidence level	99%				
Permanent FIT	2.39E-09				
Transient FIT	2.61E-09	Elevator mission profile			
Package FIT	2.20E-10				
Overall FIT	5.22E-09				
Number of units in field	1000000				
Number of device hours per day	18				
Device operating year	1	5	10	15	20
Total number of device operating year	1.00E+06	5.00E+06	1.00E+07	1.50E+07	2.00E+07
Total number of device operating hours	6.57E+09	3.29E+10	6.57E+10	9.86E+10	1.31E+11
Estimated number of failures due to Permanent fault	15.7	78.5	157.0	235.5	314.0
Estimated number of failures due to Transient fault	17.1	85.7	171.5	257.2	343.0
Estimated number of failures due to Package fault	1.4	7.2	14.5	21.7	28.9
Estimated number of failures due to Overall fault	34.3	171.5	343.0	514.4	685.9

Pessimistic estimation

Field data are orders of magnitude better

Based on RM48x v1.0 FMEDA worksheet

FMEDA worksheet – Product Function Tailoring

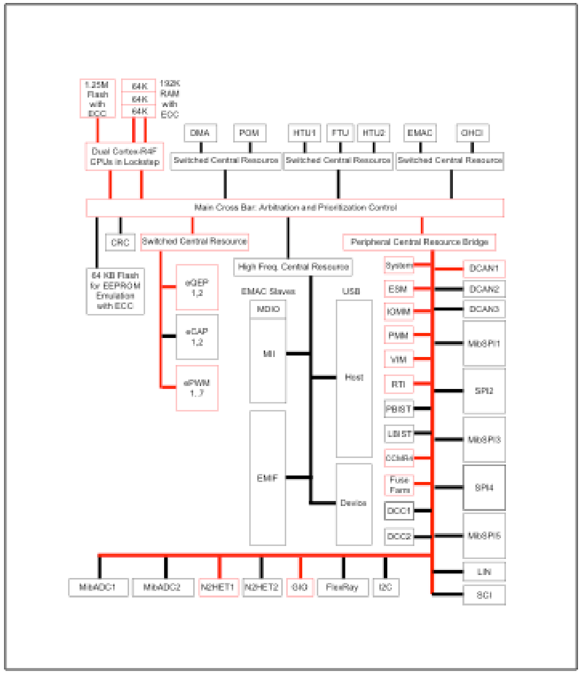
Inputs for application specific tailoring of failure rates

Memory size

Type	Total Size	User Size	Unit
SRAM	256	256	Kbytes
FLASH	3	3	Mbytes
FLASH-FEE	64	64	Kbytes

Modules used for Safety Function / Safety Goal

CPU SubSystem	Cortex R4F Central Processing Unit (CPU)	YES
CPU SubSystem	Vectored Interrupt Module (VIM)	YES
CPU SubSystem	LBIST	YES
CPU SubSystem	PBIST	YES
DEBUG	*Joint Technical Action Group (JTAG) Debug/Trace/Cali bration Access*	NO
DEBUG	*Cortex R4F Central Processing Unit (CPU) debug and trace*	NO
DEBUG	*Data Modification Module*	NO
DEBUG	*Parameter Overlay Module*	NO
DEBUG	*RAM Trace Port*	NO
RAM System	SRAM and Level 1 (L1) Interconnect	YES
Flash System	One Time Programmable (OTP) Flash Static	YES
Flash System	Primary Flash and Level 1 (L1) Interconnect	YES
Flash System	Flash emulated EEPROM (FEE)	YES
INTERCONNECT	Level 2/Level 3 (L2/L3) Interconnect	YES
SYSTEM	Error Signaling Module (ESM)	YES
SYSTEM	Power Management Module (PMM)	YES
SYSTEM	Reset	YES
SYSTEM	System Control	YES
SYSTEM	Clock	YES
SYSTEM	EFuse Static Configuration	YES
SYSTEM	Direct Memory Access (DMA)	YES
SYSTEM	Input/Output (I/O) Multiplexing (IOMM)	YES
Peripheral	*FlexRay Including FlexRay Transfer Unit (FTU)*	NO
Peripheral	Controller Area Network (DCAN1)	YES
Peripheral	Controller Area Network (DCAN2)	YES
Peripheral	Controller Area Network (DCAN3)	YES
Peripheral	General Purpose Input/Output (GIO)	YES
Peripheral	Local Interconnect Network (LIN)	YES
Peripheral	Serial Communications	YES
Peripheral	Multi-Buffered Analog to Digital Converter (MibADC1)	YES
Peripheral	Multi-Buffered Analog to Digital Converter (MibADC2)	YES
Peripheral	Multi-Buffered Serial Peripheral Interface (MibSPI1)	YES
Peripheral	Multi-Buffered Serial Peripheral Interface (MibSPI3)	YES
Peripheral	Multi-Buffered Serial Peripheral Interface (MibSPI5)	YES
Peripheral	Next Generation High End Timer (N2HET1) Including HET Transfer Unit (HTU1)	YES
Peripheral	Next Generation High End Timer (N2HET2) Including HET Transfer Unit (HTU2)	YES
Peripheral	Serial Peripheral Interface (SPI2)	YES
Peripheral	Serial Peripheral Interface (SPI4)	YES
Peripheral	Real Time Interrupt (RTI) Operating System Timer	YES
Peripheral	Ethernet	YES
Peripheral	External Memory Interface (EMIF)	YES
Peripheral	Universal Serial Bus (USB)	YES
Peripheral	Inter-Integrated Circuit (I2C)	YES
Power Supply	Power Supply	YES
Package	Package	YES



- Allow customization of failure rate estimation
  - Include only MCU modules used by application
  - Include actual Flash and SRAM memory size used

FMEDA worksheet – Safety Mechanisms Tailoring

Safety mechanisms considered in the FMEDA

From TI Safety Manual				
Device Partition	**Unique identifier**	**Safety Feature or Diagnostic**	**Feature Reccomendation**	**Diagnostic Used in Application?**
Power Supply	PWR1	Voltage monitor (VMON)	M	1
Power Supply	PWR2	External voltage supervisor	++	1
Power Management Module (PMM)	PMM1	Lockstep PSCON	M	1
Power Management Module (PMM)	PMM2	Privileged Mode Access and Program Sequence Control Registers	M	1
Power Management Module (PMM)	PMM3	Periodic SW readback of static configuration registers	+	1
Power Management Module (PMM)	PMM4	SW readback of written configuration	++	1
Power Management Module (PMM)	PMM5	PSCON lockstep compare self-test	++	1
Clock	CLK1	LPOCLKDET	++	1
Clock	CLK2	PLL slip detector	++	1
Clock	CLK3	Dual Clock Comparator (DCC)	++	1
Clock	CLK4	External monitoring via ECLK	O	0
Clock	CLK5A	Internal watchdog -DWD	O	0
Clock	CLK5B	Internal watchdog -DWWD	+	0
Clock	CLK5C	External watchdog	++	1
Clock	CLK6	Periodic SW readback of static clock configuration registers	+	1
Clock	CLK7	SW readback of written configuration	++	1
Reset	RST1	External monitoring of warm reset	O	0
Reset	RST2	SW check of last reset	++	1
Reset	RST3	SW warm reset generation	O	0
Reset	RST4	Glitch filtering on reset pins	M	1
Reset	RST5	Use of status shadow registers	++	1
Reset	RST6	External watchdog	++	1
Reset	RST7	Periodic SW readback of static configuration registers	+	1
Reset	RST8	SW readback of written configuration	++	1

Device Partition	Unique identifier	Safety Feature or Diagnostic	Feature Reccomendation	Diagnostic Used in Application?
Cortex R4F Central Processing Unit (CPU)	CPU1	Lockstep compare	M	1
Cortex R4F Central Processing Unit (CPU)	CPU2A	Boot time execution of LBIST STC	++	1
Cortex R4F Central Processing Unit (CPU)	CPU2B	Periodic execution of LBIST STC	O	0
Cortex R4F Central Processing Unit (CPU)	CPU3	MPU	++	1
Cortex R4F Central Processing Unit (CPU)	CPU4	Online profiling using PMU	O	0
Cortex R4F Central Processing Unit (CPU)	CPU5A	Internal watchdog -DWD	O	0
Cortex R4F Central Processing Unit (CPU)	CPU5B	Internal watchdog -DWDD	+	0
Cortex R4F Central Processing Unit (CPU)	CPU5C	External watchdog	++	1
Cortex R4F Central Processing Unit (CPU)	CPU6	Illegal operation and instruction trapping	++	1
Cortex R4F Central Processing Unit (CPU)	CPU7	SW readback of written configuration	++	1
Cortex R4F Central Processing Unit (CPU)	CPU8	Lockstep compare (CCM) self-test	++	1
Primary Flash and Level 1 (L1) Interconnect	FLA1	Flash Data ECC	++	1
Primary Flash and Level 1 (L1) Interconnect	FLA2	Hard error cache and livelock	M	1
Primary Flash and Level 1 (L1) Interconnect	FLA3	Flash wrapper address ECC	++	1
Primary Flash and Level 1 (L1) Interconnect	FLA4	Address parity	++	1
Primary Flash and Level 1 (L1) Interconnect	FLA5A	Boot time hardware CRC check of flash memory contents	++	1
Primary Flash and Level 1 (L1) Interconnect	FLA5B	Periodic hardware CRC check of flash memory contents	+	1
Primary Flash and Level 1 (L1) Interconnect	FLA6	Bit multiplexing in flash array	M	1
Primary Flash and Level 1 (L1) Interconnect	FLA7	Flash sector protection	++	1
Primary Flash and Level 1 (L1) Interconnect	FLA8	Periodic SW readback of static configuration registers	+	1
Primary Flash and Level 1 (L1) Interconnect	FLA9	SW readback of written configuration	++	1

- Allow customization of diagnostics selection.
- For example, CPU lock-step compare and boot time LBIST are used, while periodic LBIST is not used.

FMEDA worksheet – Package/Pin Tailoring

Pin	Number of pins (PBGA)	Number of pins (QFP)	Safety related 1=YES, 0=NO	Related Part
ADREFHI	1	1	1	Multi-Buffered Analog to Digital Converter
ADREFLO	1	1	1	Multi-Buffered Analog to Digital Converter
VCCAD	1	1	1	Multi-Buffered Analog to Digital Converter
VSSAD	4	1	1	Multi-Buffered Analog to Digital Converter
AD1EVT	1	1	1	Multi-Buffered Analog to Digital Converter
AD2EVT	1	1	1	Multi-Buffered Analog to Digital Converter
AD1IN	8	8	1	Multi-Buffered Analog to Digital Converter
AD1IN/AD2IN	16	16	1	Multi-Buffered Analog to Digital Converter
NHET1	31	31	1	Enhanced High-End Timer Modules (NHET)
NHET2	18	9	1	Enhanced High-End Timer Modules (NHET)

Diagnostic Coverage of customer safety mechanisms	SM	on / off	Diagnostic Coverage of customer safety mechanisms	SM	on / off	RESULTING DIAGNOSTIC COVERAGE
0.000%	-	0	0.000%	-	0	99.990%
0.000%	-	0	0.000%	-	0	99.990%
0.000%	-	0	0.000%	-	0	99.990%
0.000%	-	0	0.000%	-	0	99.990%
0.000%	-	0	0.000%	-	0	99.990%
0.000%	-	0	0.000%	-	0	99.990%
0.000%	-	0	0.000%	-	0	99.000%
0.000%	-	0	0.000%	-	0	99.000%
0.000%	-	0	0.000%	-	0	99.990%
0.000%	-	0	0.000%	-	0	99.990%

Allow customer to adjust the number of pins used by module in its application

- Example: 31 NHET1 pins are available, if only 20 pins are used, change to 20

Allow customer to input pin-level application diagnostic with its own diagnostic coverage number

FMEDA worksheet – Metrics Summary / Details

Summary of IEC 61508 Metrics Examples – Permanent/Transient & Die/Package:

Numbers are normalized to Die Permanent Total RAW FIT

	Die		Package	Overall
	Permanent	Transient	Permanent	Sum
Total FIT (Raw FIT)	10.00	764.40	69.89	844.30
Safety related FIT	9.97	734.58	68.95	813.49
Probability of Hardware Failures - PFH (in FIT)	0.06	0.82	0.13	1.01
Safe Failure Fraction - SFF	99.36%	99.89%	99.82%	99.88%

IEC 61508 categorization

		Die		Package	Overall
		Permanent	Transient	Permanent	Sum
Total faults	λ	10.00	764.40	69.89	844.30
Total non safety related faults	λ_{nSR}	0.03	29.83	0.94	30.80
Total Safe faults	λ_S	5.24	372.78	34.47	412.50
Total dangerous faults	λ_D	4.73	361.79	34.47	401.00
Total dangerous Detected faults	λ_{DD}	4.67	360.97	34.35	399.99
Total dangerous UnDetected faults	λ_{DU}	0.06	0.82	0.13	1.01

Details of IEC 61508 Metrics:

- For Permanent and Transient faults
- By modules (CPU, Flash, SRAM, DCAN, ADC…)

Component level	Device Partition (according to TI SM)
CPU SubSystem	Cortex R4F Central Processing Unit (CPU)
CPU SubSystem	Vectored Interrupt Module (VIM)
CPU SubSystem	LBIST
CPU SubSystem	PBIST
DEBUG	Joint Technical Action Group (JTAG) Debug/Trace/Calibration Access
DEBUG	Cortex R4F Central Processing Unit (CPU) debug and trace
DEBUG	Data Modification Module
DEBUG	Parameter Overlay Module
DEBUG	RAM Trace Port
RAM System	SRAM and Level 1 (L1) Interconnect
Flash System	One Time Programmable (OTP) Flash Static
Flash System	Primary Flash and Level 1 (L1) Interconnect
Flash System	Flash emulated EEPROM (FEE)
INTERCONNECT	Level 2/Level 3 (L2/L3) Interconnect
SYSTEM	Error Signaling Module (ESM)
SYSTEM	Power Management Module (PMM)
SYSTEM	Reset
SYSTEM	System Control
SYSTEM	Clock
SYSTEM	EFuse Static Configuration
SYSTEM	Direct Memory Access (DMA)
SYSTEM	Input/Output (I/O) Multiplexing (IOMM)
Peripheral	FlexRay including FlexRay Transfer Unit (FTU)
Peripheral	Controller Area Network (DCAN1)
Peripheral	Controller Area Network (DCAN2)
Peripheral	Controller Area Network (DCAN3)
Peripheral	General Purpose Input/Output (GIO)
Peripheral	Local Interconnect Network (LIN)
Peripheral	Serial Communications
Peripheral	Multi-Buffered Analog to Digital Converter (MibADC1)
Peripheral	Multi-Buffered Analog to Digital Converter (MibADC2)
Peripheral	Multi-Buffered Serial Peripheral Interface (MibSPI1)
Peripheral	Multi-Buffered Serial Peripheral Interface (MibSPI3)
Peripheral	Multi-Buffered Serial Peripheral Interface (MibSPI5)

Permanent faults Failure Rate, FIT (high demand)

Raw Permanent faults FIT	Failure rate to be excluded from the analysis (no effect or no part)	Safety Related failure rate	DU	DD	S	PFH
2.70E-02	0.00E+00	2.70E-02	1.09E-05	6.82E-03	2.02E-02	1.09E-05
2.67E-03	0.00E+00	2.67E-03	7.31E-06	1.32E-03	1.34E-03	7.31E-06
2.28E-01	0.00E+00	2.28E-01	2.61E-07	1.60E-06	2.28E-01	2.61E-07
3.47E-02	0.00E+00	3.47E-02	8.53E-06	0.00E+00	3.47E-02	8.53E-06

Alpha + Neutron Transient faults Failure Rate, FIT

Raw Transient faults FIT Total of Alpha + Neutron	Failure rate to be excluded from the analysis (no effect or no part)	Safety Related failure rate	DU	DD	S	PFH
9.71E+00	0.00E+00	9.71E+00	2.19E-03	2.20E+00	7.50E+00	2.19E-03
1.32E+00	0.00E+00	1.32E+00	9.94E-03	6.34E-01	6.72E-01	9.94E-03
7.47E-01	0.00E+00	7.47E-01	4.30E-05	4.25E-03	7.42E-01	4.30E-05
1.28E+00	0.00E+00	1.28E+00	5.68E-04	0.00E+00	1.28E+00	5.68E-04

Based on RM48x v1.0 FMEDA worksheet

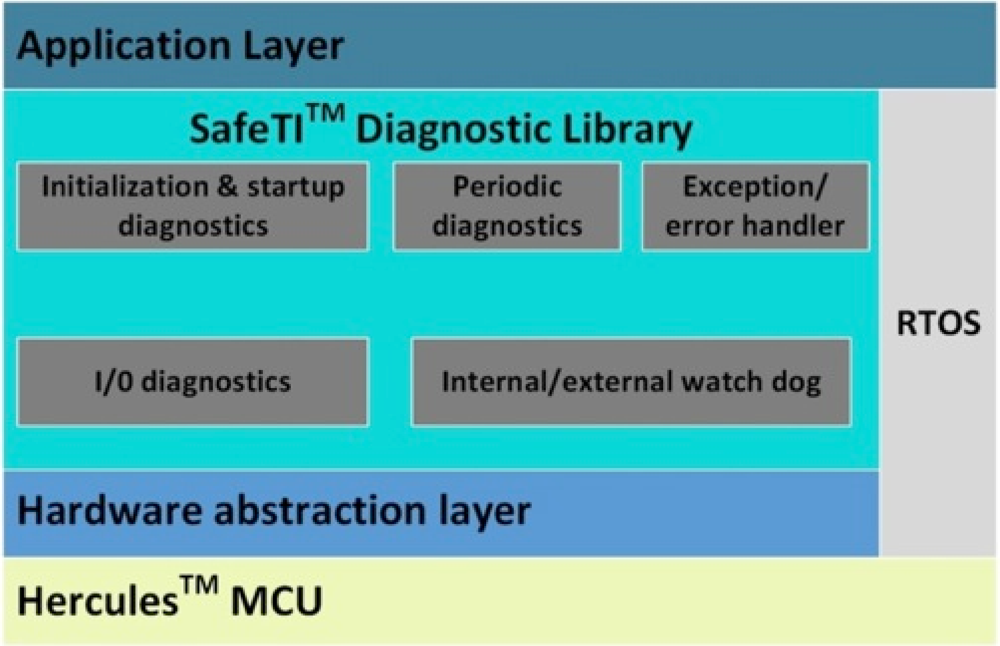
Agenda

- Overview of Hercules™ MCU and SafeTI™ Design package
- Hercules™ MCU Functional Safety How-To Workshop
  - Safety Functions, Safety Goals, Safe State, SIL, Failure rate
  - Safety Critical Elements identification and Diagnostic Requirements
  - Safety Manual and Diagnostics Selection
  - Mission Profile and Failure Rate Estimation
  - SafeTI™ Diagnostic Library
  - SafeTI™ Diagnostic Library Compliance Support Package (CSP) certification support
  - Fault Injection with HITEX kit
- Summary

Hercules™ SafeTI™ Diagnostic library

- SafeTI™ Diagnostic Library = **Executable version of Safety Manual**.

- Highlights
  - Optimized API mapping to the MCU's Safety features as documented in the device Safety Manual.
  - Software abstraction for MCU's Safety features to an application developer.
  - Uniform API across various members of the Hercules family.
  - Developed compliant to an ISO26262 and IEC61508 development process.



Hercules™ SafeTI™ Diagnostic Library features

- **Initialization** functions for the device
  - Common functionality (Core registers, stack)
  - Safety measures (RAM init, enable ECC, ESM init)
- API to **invoke PBIST** on memories.
- API to **invoke LBIST** self tests.
- **Boot time/Run time verification** of integrated HW safety diagnostics to prevent latent faults.
- Create artificial faults (**Fault injection**) to allow testing of application fault handling.
- Provide an **Error Signaling Module (ESM) handler** which can capture and report faults to the application through a **callback** routine.
- **Profiling** for measuring time spent in diagnostic tests/fault handling, for enabling optimization of Run time safety measures by application developer.
- **Comprehensive documentation** which explains mapping from Safety manual to SafeTI™ Diagnostic Library API.
- Released in a **SafeTI™ Software Compliance Support Package (SCSP)** which aids in ISO26262 or IEC61508 certification of customer product.
- Current implementation is limited to "safe island" set of peripherals.

Safety Manual to API mapping

SafeTI™ Diagnostic Library 1.0.0

SafeTI™ Diagnostic Library for the Hercules processors

Main Page | Related Pages | Modules | Data Structures | Files

Safety manual to API mapping

Device Partition	Unique Identifier	Safety Feature or Diagnostic	API Name	Remarks
Power Supply	PWR1	Voltage monitor (VMON)	Not applicable	No software control,always enabled in hardware
	PWR2	External voltage supervisor	Not applicable	External monitoring
Power Management Module (PMM)	PMM1	Lockstep PSCON	SL_SelfTest_PSCON	
	PMM2	Privileged mode access and multi-bit keys for control registers	SL_SelfTest_PSCON	
	PMM3	Periodic software readback of static configuration registers	SL_Read_Compare	
	PMM4	Software readback of written configuration	SL_Read_Compare	
Clock	CLK1	LPOCLKDET	Not applicable	External source for fault
	CLK2	PLL slip detector	ESM_Application_Callback	
	CLK3	Dual Clock Comparator (DCC)	ESM_Application_Callback	
	CLK4	External monitoring via ECLK	Not applicable	External monitoring
	CLK5A	Internal watchdog - DWD	Not applicable	External source for fault
	CLK5B	Internal watchdog - DWWD	Not applicable	External source for fault
	CLK5C	External watchdog	Not applicable	External monitoring
	CLK6	Periodic software readback of static clock configuration registers	SL_Read_Compare	
	CLK7	Software readback of written configuration	SL_Read_Compare	
Reset	RST1	External monitoring of warm reset	Not applicable	External monitoring
	RST2	Software check of last reset	SL_Init_ResetReason	
	RST3	Software warm reset generation	SL_SW_Reset	
	RST4	Glitch filtering on reset pins	Not applicable	No software control,always enabled in hardware
	RST5	Use of status shadow registers	SL_Init_ResetReason_XInfo	

Hercules MCU safety features and SafeTI™ Diagnostic Library

Many API also provide a "fault injection" mode

- •API for running LBIST on the CPU by the STC.
- •API also supports selfcheck feature of STC, which tests the signature compare logic .

- •API to perform test on the ECC diagnostic feature.
- •API to run the diagnostic modes on Flash memories.
- •API to perform CRC calculation on memory ranges.

- •API to run PBIST algorithms on all memories.

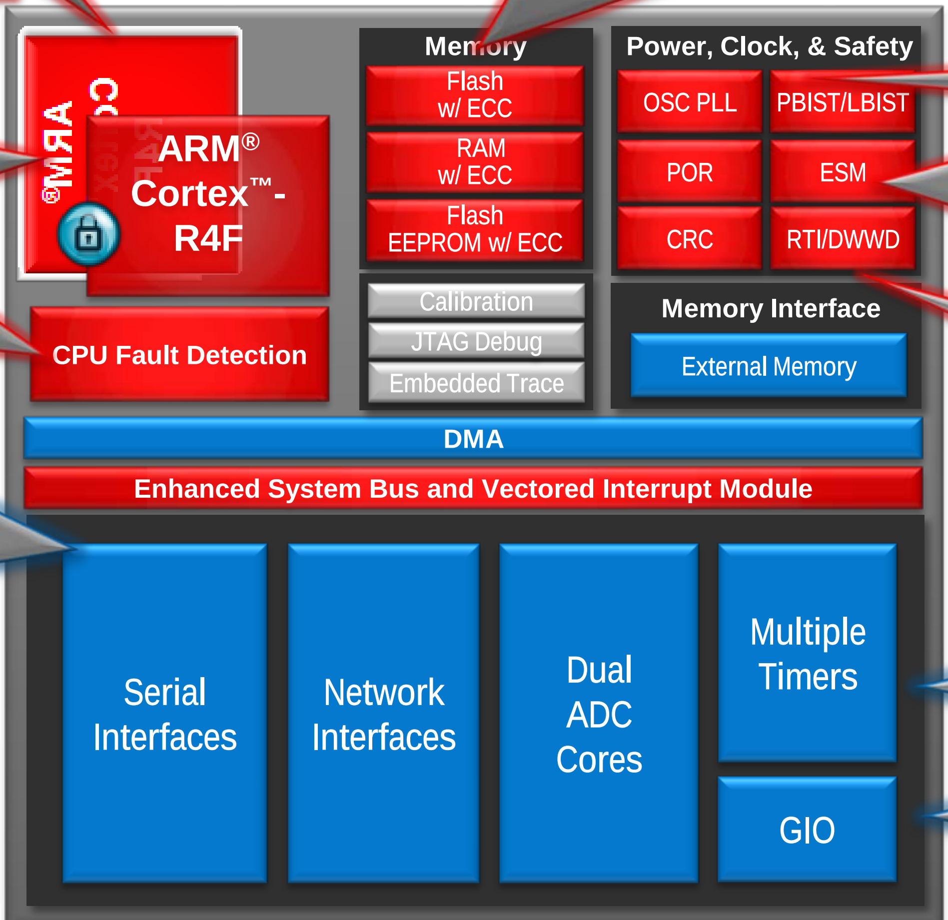
Logical / physical design optimized to reduce probability of common cause failure

- •Includes ESM handler and provides an example application with an abort handler.
- •Allows application to register a callback for the fault handling

- •API to test the CCM Diagnostic feature.
- •API to test error forcing capabilities of the CCM

- •On-Chip Clock and Voltage Monitoring
- •API for testing the safety diagnostics on PSCON.
- •API for testing the safety diagnostics on EFUSE.

- •API's to test the parity diagnostics for peripheral memories and perform SRAM data parity fault injections
- •API to perform CRC calculation on memory ranges.



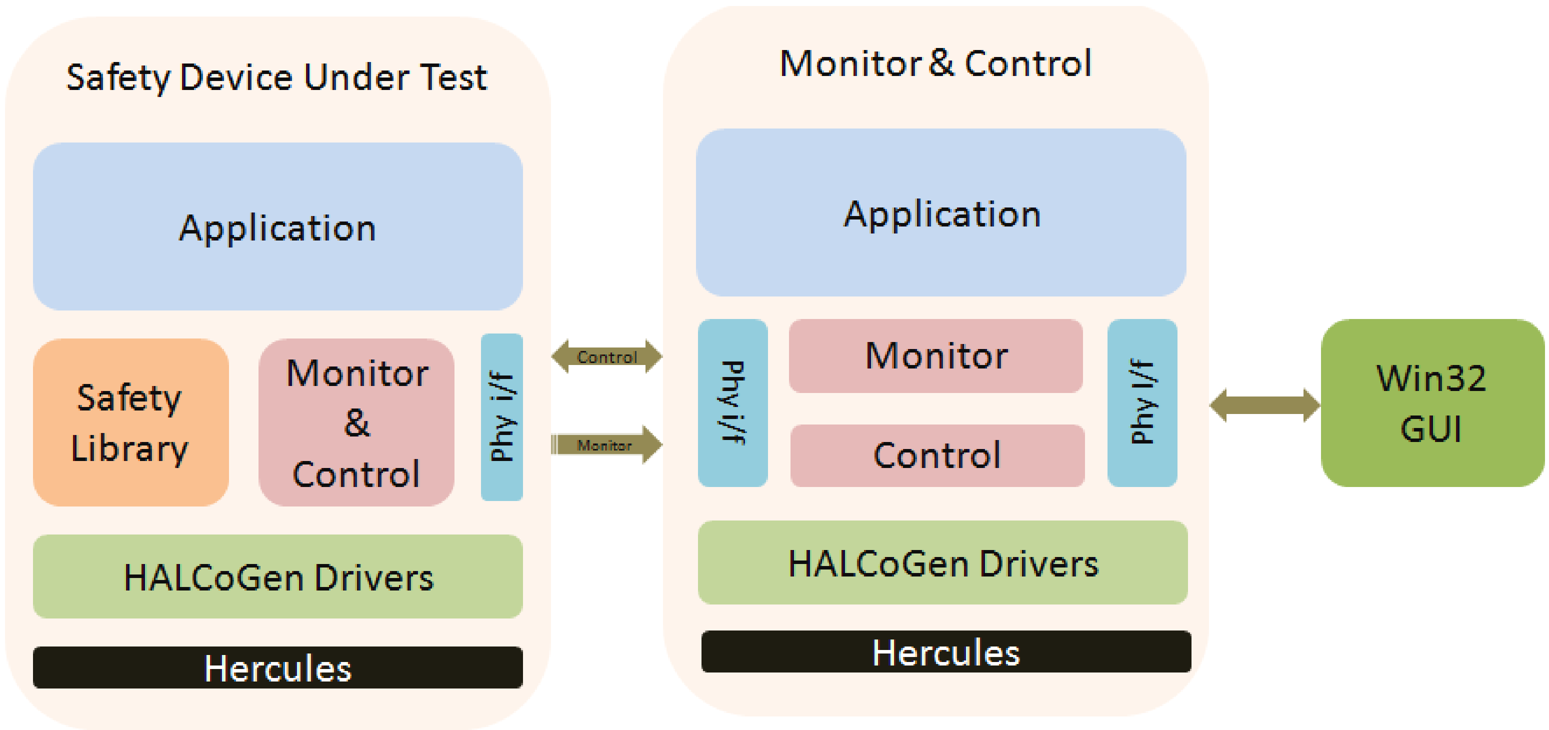
- •IO Loop Back, ADC Self Test, …

Dual ADC Cores with shared channels

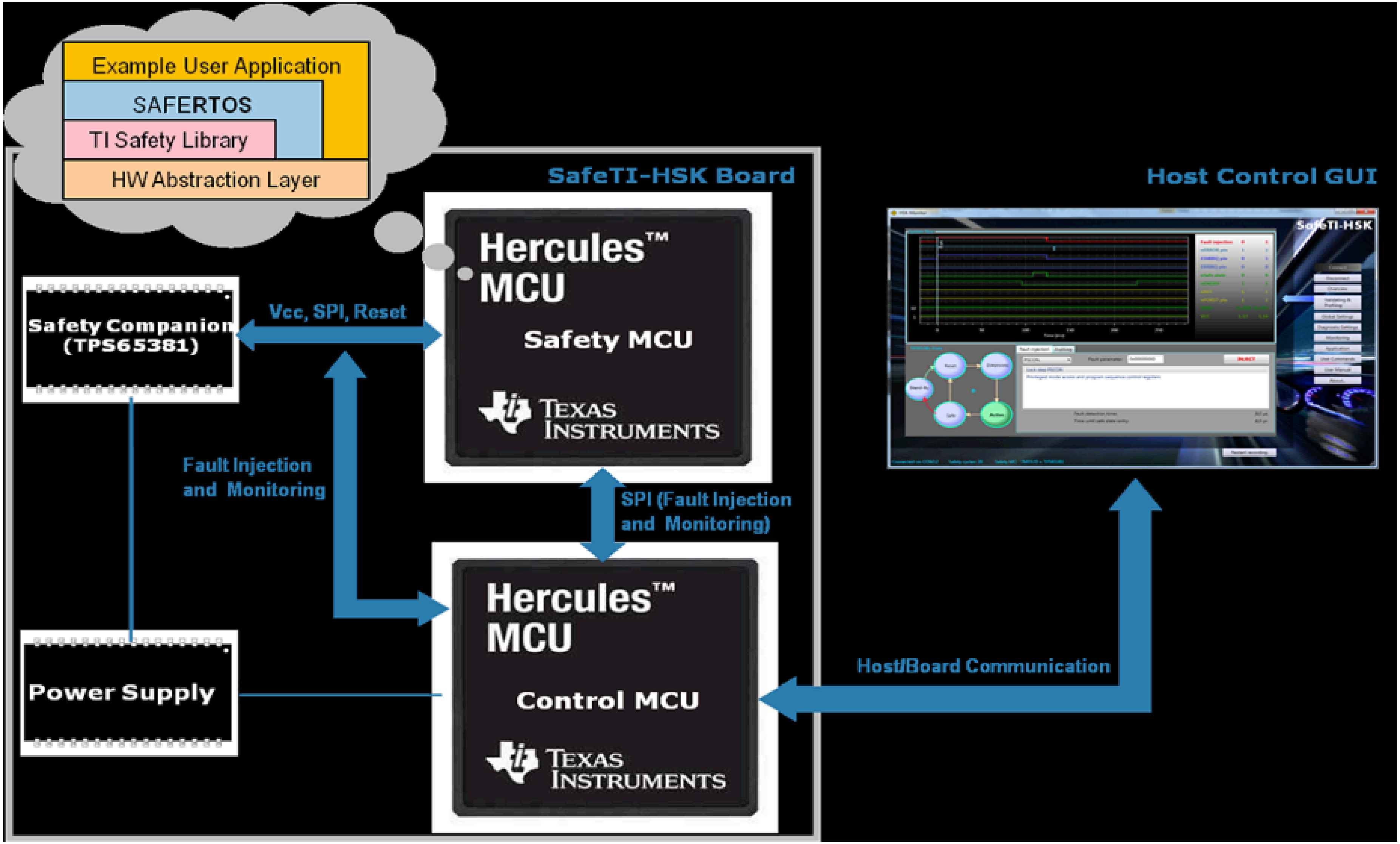
- Safe Island Hardware diagnostics (RED)
- Blended HW diagnostics (BLUE)
- Non Safety Critical Functions (BLACK)

User examples

- SafeTI™ Diagnostic Library is integrated into the Hitex Safety Kit.



Hitex Kit



Example User Application
SAFERTOS
TI Safety Library
HW Abstraction Layer
SafeTI-HSK Board
Host Control GUI
Safety Companion (TPS65381)
Vcc, SPI, Reset
Hercules™ MCU
Safety MCU
Texas Instruments
Fault Injection and Monitoring
SPI (Fault Injection and Monitoring)
Power Supply
Hercules™ MCU
Control MCU
Texas Instruments
Host/Board Communication
SafeTI-HSK

Agenda

- Overview of Hercules^{TM} MCU and SafeTI^{TM} Design package
- Hercules MCU Functional Safety How-To Workshop
  - Safety Functions, Safety Goals, Safe State, SIL, Failure rate
  - Safety Critical Elements identification and Diagnostic Requirements
  - Safety Manual and Diagnostics Selection
  - Mission Profile and Failure Rate Estimation
  - SafeTI^{TM} Diagnostic Library
  - SafeTI Diagnostic Library Compliance Support Package (CSP) certification support
  - Fault Injection with HITEX kit
- Summary

Hercules™ and SafeTI™ Software and Tool Packages

Hercules Software and Tools

FREE!!

Hercules standard software and tools packages

- ➢ Assists in software development on Hercules Safety MCUs
- ➢ Provides the actual software/tool with source code, GUI, …
- ➢ User guides, datasheets, release notes, …
- ➢ Regular updates for enhancements, fixes, …

Free / click wrap license agreement

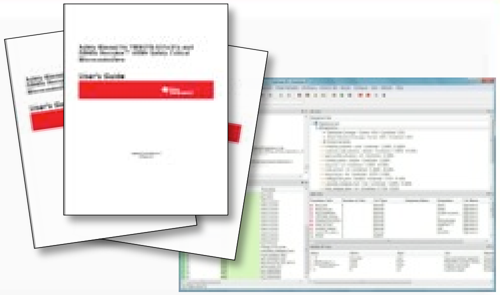


SafeTI Compliance Support Package

SafeTI software documentation and testing

- ➢ Assists customer to comply to functional safety standards
- ➢ Safety Requirements Document, Code Review and Coverage Reports, Unit Test Results, Software Safety Manual, ….
- ➢ Unit Test capability using LDRAunit (if applicable)

See Pricing / signed license agreement

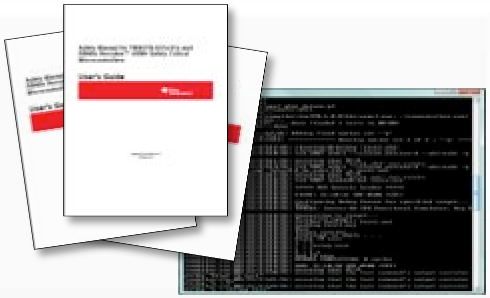


SafeTI Tool Qualification Kit

SafeTI tool documentation and qualification

- ➢ Assists customer to qualify tool to functional safety standards
- ➢ Tool Classification Report, Tool Qualification Plan and Report, Tool Safety Manual, …
- ➢ TI Test Automation Unit or LDRAunit (if applicable)

See pricing / signed license agreement



Hercules Software and Tool Packages

Standard Package	Compliance Support Package	Tool Qualification Kit
Code in source form (see note)	Software Safety Requirements Document	Tool Safety Requirements Document
GUI for user configuration (if applicable)	Software Safety Architecture Document	Tool Safety Architecture Document
Software/Tool user guide	Code Review Report (w/ MISRA-C)	Code Review Report (w/ MISRA-C)
Data sheet	Quality Review Report	Quality Review Report
Release notes	Dynamic Coverage Analysis Report	Dynamic Coverage Analysis Report
	Unit Test Regression Report	Unit Test Regression Report
	Traceability report	Traceability report
	Test Results Report	Test Results Report
	Software Safety Manual	Tool Safety Manual
	Safety Assessment Report (Internal)	Safety Assessment Report (Internal)
		Compliance Level Tool
		Templates for Compliance Documentation
	Executable Test Cases*	**Executable Test Cases***
Click Wrap License	**Signed License Agreement**	**Signed License Agreement**
Free	**See Pricing Table**	**See Pricing Table**

** - these are provided for software that is configurable by user (ie; HALCoGen and CCS Compiler)*

SafeTI™ Compliance Support Packages

Following artifacts are provided as part of a SafeTI™ Compliance Support Package:

1. **Software/Tool Safety Requirements document**
   - ❑ Defines both functional and safety requirements of the software/tool
2. **Software/Tool Safety Architecture Document**
   - ❑ Defines the architecture of the software/tool including safety provisions
3. **Code Review Report**
   - ❑ Provides the MISRA-C:2004 violations for the file
4. **Quality Review Report**
   - ❑ Provides the HIS Quality metrics for the file.
5. **Dynamic Coverage Analysis Report**
   - ❑ Provides the Statement, Branch, and MC/DC Coverage information
6. **Unit Test Regression Report**
   - ❑ Shows the unit tests performed and the result of each unit test.
7. **Test Manager report**
   - ❑ Summary of the Code Review, Quality Review and Unit Test Reports.

SafeTI™ Compliance Support Packages

8. **Test Results Report**
   - ❑ unit tests
   - ❑ safety functional tests
   - ❑ performance tests/resource usage tests
   - ❑ interface tests
   - ❑ fault injection tests
9. **Traceability report**
   - ❑ requirements to design
   - ❑ requirements to source code
   - ❑ requirements to test case
   - ❑ backwards traceability
10. **Software Safety Manual**
    - ❑ describes how to integrate safely into end user application software
11. **ISO 26262 / IEC 61508 assessment report**
    - ❑ shows review of entire development process (internal assessment)
12. **Executable test cases (HALCoGen only)**
    - ❑ setup for user defined configuration
13. **Test Automation Unit (HALCoGen only)**
    - ❑ for executing unit tests with user defined configuration

Software Compliance Support Package Deliverables

ISO 26262 and IEC61508 Standards				TI Work Products	TI SW Product Lifecycle						
ISO 26262 Clause	IEC 61508 Clause	ISO 26262 Work products	IEC61508 Work products	Customer Deliverable	Generic Inputs- (Can modify during project tailoring)	CP1-Project Commissioning	CP2- Safety Requirements & Planning	CP3A- Design & Implementation	CP3B- Unit Testing & Integration Testing	CP4- Safety Requirements Verification & Release	CP5- Project Closure
6 Specification of software safety requirements	7.2.2 Software safety requirements specification	6.5.1 Software safety requirements specification	Software safety requirements specification	Software Requirements Document			X				
Bi-Directional Traceability	Forward and Backward Traceability at all stages	Verification Reports	Forward and backward traceability	Traceability matrix			X				
7 Software architectural design	7.4.3 Requirements for SW Architecture Design development	7.5.1 Software architectural design specification	software architecture design;	SW Architecture Spec				X			
9 Software unit testing	7.4.5 Detailed design and development (individual software module design):	9.5.3 Software verification report (refined)	SW Module Test Report	Unit Test & Static Analysis Report, Dynamic Coverage Analysis Report, Test Manager Report					X		
10 Software integration and testing	7.4.8 Software integration testing:	10.5.3 Embedded software	verified and tested integrated programmable electronics	SW User Guide, Software Safety Manual, Data sheet					X	X	
11 Verification of software safety requirements	7.7.2 Software aspects of system safety validation	11.5.3 Software verification report (refined)	software safety validation results; validated software	Safety Test Report						X	
	7.4.9- Safety Manual		Safety Manual	SW Manual						X	
6.4.9 Safety Assessment	Software functional 8 safety assessment	Functional Safety Assessment Plan Functional Safety Assessment Report	software functional safety assessment plan software functional safety assessment report	Functional Safety Assessment Plan in Safety, Plan, Functional Safety Assessment Report	X	X	X	X	X	X	X

Agenda

- Overview of Hercules™ MCU and SafeTI™ Design package
- Hercules™ MCU Functional Safety How-To Workshop
  - Safety Functions, Safety Goals, Safe State, SIL, Failure rate
  - Safety Critical Elements identification and Diagnostic Requirements
  - Safety Manual and Diagnostics Selection
  - Mission Profile and Failure Rate Estimation
  - SafeTI™ Diagnostic Library
  - SafeTI™ Diagnostic Library Compliance Support Package (CSP) certification support
  - Fault Injection with HITEX kit
- Summary

The SafeTI™- HSK Hardware

HSK hardware platform:

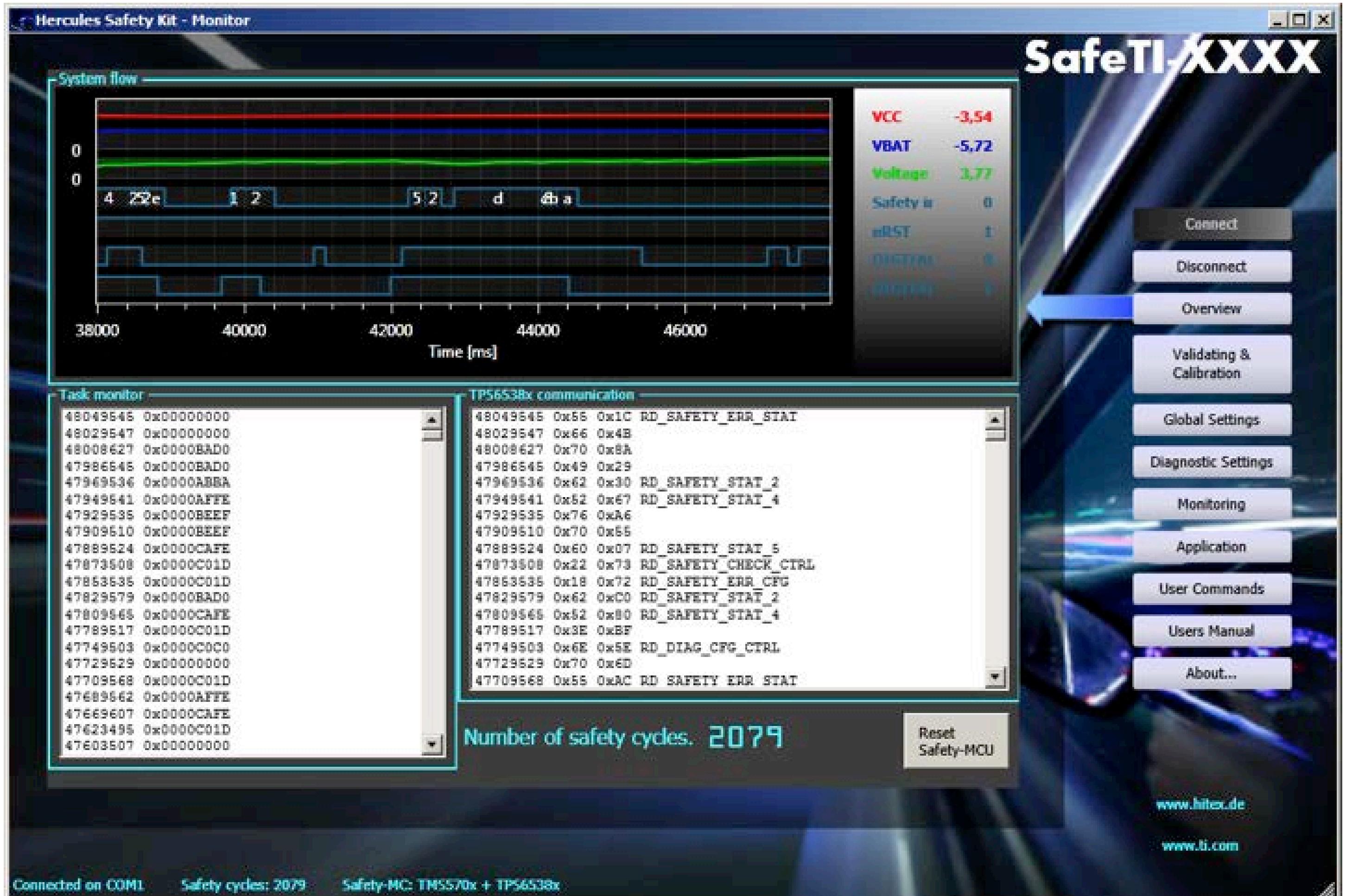
- **Safety application unit** on which the Demo application is run. This includes The Safety MCU or Safety Device Under Test(SDUT) -- TMS570 or RM48, Power supply/WD companion chip (TPS65381), Accelerometer, Temperature Sensor, HMI (4XLED, potentiometer, Pixel display..), CAN (transceiver & connector) and motor control interface (DIMM connector)
- **Control and Monitoring unit(CMU)** : This includes the control and monitor device (RM48x) to inject faults and monitor fault reaction, Fault injection logic, Error indication and power supply to the control monitor unit
- **Host/Debug interface**: This includes a USB HUB controller (to manage USB communication between the Host workstation and onboard MCU's) and Serial communication port converters (FTDI) from the USB HUB to the Safety DUT (JTAG) and CMU device (JTAG and UART(for the GUI))
- The board utilizes an industry standard **DIMM** form factor. Uses the standard 100-pin connector foot print to plug into selected TI's motor control kits
- Standard 20 pin external JTAG header to facilitate expandability Non-CCS IDE's like IAR and Keil

The SafeTI™- HSK GUI

- Communicates permanently with the kit to request status information
- Monitors different voltages of power supply ranges
- Possibilty to inject faults (disturb power supply or simulate errors in the appication)
  The system reaction is monitored with timestamps (fault injection, fault indication, enter safe-state)
- Measure runtime execution of safety tests. This gives the user a clear picture how to configure or calibrate his application
- Ability to configure settings for Error Signalling Module and TPS6538x
- Application information is visualized e.g. acceleration, temperature and some task state information

The SafeTI™- HSK GUI Overview

- GUI overview



The SafeTI™- HSK GUI Validation and Calibration



The SafeTI™- HSK
CPU Lock-Step Compare Fault Injection

- CCM-R4F compares the outputs of two CPUs running in a 1oo1D lockstep configuration
- The ESM error flag “CCM-R4F - compare” is asserted whenever the CPU compare error is detected.
- For diagnostic purposes, the CCM-R4F also incorporates a self-test capability and error forcing capability.
- FMEDA requires gate-level fault injection (simulation) work to prove effectiveness of on chip diagnostics

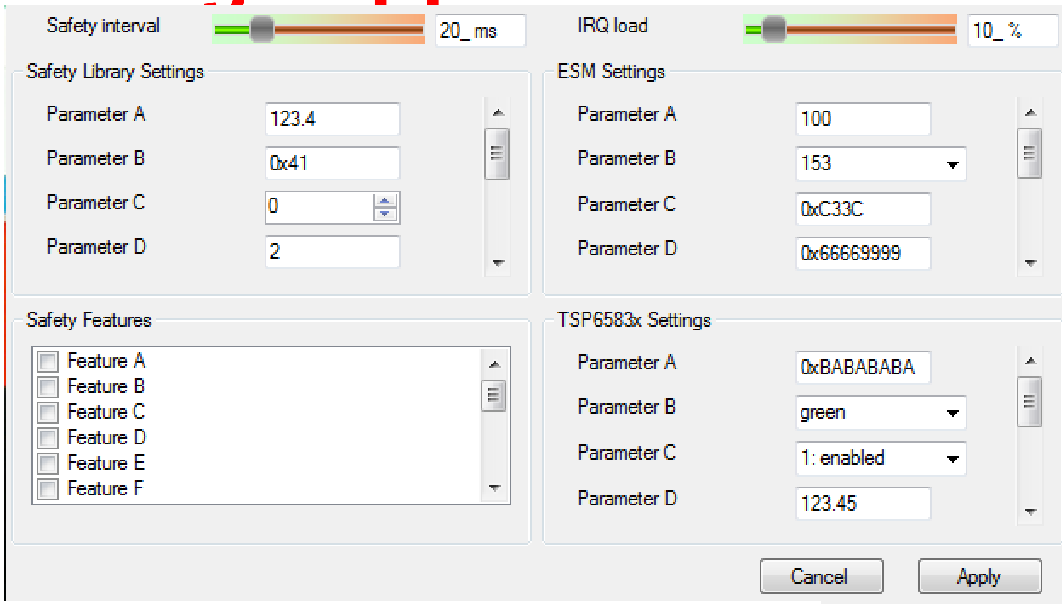


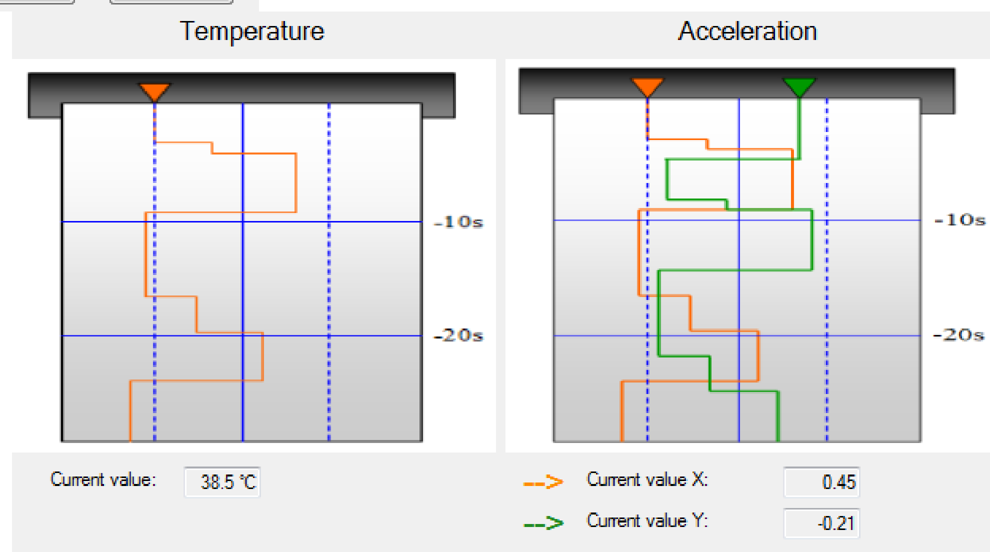
The SafeTI™- HSK
SRAM DATA ECC Fault Injection

- ECC controllers are located inside the CPU
  – Interconnect between CPU and the memory is covered by the diagnostic
  – ECC logic itself is checked on a cycle by cycle basis
  – Single Error Correction Double Error Detection (SECDED) logic
- 8 bits of ECC for every 64 bits of data access from the CPU



The SafeTI™- HSK GUI settings/application





Agenda

- Overview of Hercules™ MCU and SafeTI™ Design package
- Hercules™ MCU Functional Safety How-To Workshop
  - Safety Functions, Safety Goals, Safe State, SIL, Failure rate
  - Safety Critical Elements identification and Diagnostic Requirements
  - Safety Manual and Diagnostics Selection
  - Mission Profile and Failure Rate Estimation
  - SafeTI™ Diagnostic Library
  - SafeTI™ Diagnostic Library Compliance Support Package (CSP) certification support
  - Fault Injection with HITEX kit
- Summary

Hercules MCUs: Accelerating Safety Products to Market

Hercules™ Safety MCU

Texas Instruments

Broad Eco-system
- Software
- Development Tools
- Consulting & Training

Certified Safety Hardware Architecture
- Pre-approved for ISO 26262, IEC 61508
- Proven in use
- Device FMEDA, FIT reports

Unique Tools for Safety Development
- Ease development
- Aid certification

Only Lockstep ARM supplier
- Non-proprietary
- Market accepted
- Respected heritage

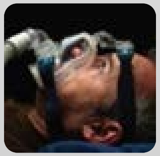
Production Quality Safety Software
- Usable by customer
- Certification Ready
- ISO 26262, IEC 61508 compliant

Comprehensive Portfolio
Complementary Analog
- Pin & SW Compatible
- Safety Chipset
- SafeTI Program









Hercules™ Training www.ti.com/herculestraining



1 Day Training Class:
Hercules 1 Day Safety Seminar

- Introduction
- What is Functional Safety?
- Safety Standards Overview
- IEC 61508 Safety Standard
- ISO 26262 Safety Standard
- Random Fault Management
- Safety System Architectures
- Hercules Safety Concept
- *Lab 1*: Hercules MCU Demos
- Hercules Architecture
- Development Tools: HW kits, SW tools
- Embedded Flash Memory tools
- Real Time Interrupt (RTI)
- Vectored Interrupt Manager (VIM)
- Direct Memory Access (DMA)
- General-purpose I/O (GIO) & NHET
- *Lab 2*: Using NHET as GIO
- Communication Interfaces: UART, LIN, CAN, FlexRay, Multi-Buffered Serial Peripheral Interface (MibSPI)
- *Lab 3*: PC to SCI Communication
- External Memory Interface (EMIF) / Parameter Overlay
- Multi-buffered Analog-to-Digital Converter (MibADC)
- Support Structure: Web, Forum, WIKI

3 Day Training Class:
Safety Critical Design and Programming with ARM® Cortex®-R4F based Hercules MCUs

Who should attend:
- Hardware and Software Developers
- Project Managers
- Safety Specialists
- Anyone interested in Hercules MCUs and functional safety

Day 1
- Welcome and Intro
- Hercules Product Overview / MCU Roadmap
- Safety Standards and Hercules Safety Features
- HALCoGen / Exercise
- Code Composer Studio / Demonstration / Exercise
- Compiler / Exercise
- Flash Overview
- Flash Tools: nowFlash™, nowECC™, nowProfile™

Day 2
- Summary / Questions
- ARM ® Cortex®-R4F CPU Architecture Overview
- System Module Overview
- Device setup/startup, Real Time Interrupt Module, Vectored Interrupt Manager
- CRC Controller, CPU Compare Module, Error Signaling Module)
- General Purpose I/Os / Supply
- Direct Memory Access Controller (DMA)
- Serial Communication Interface (SCI/UART/LIN)

Day 3
- Summary / Questions
- Multi-Buffer Serial Peripheral Interface (SPI / MIBSPI-P)
- DCAN
- FlexRay / Transfer Unit
- Multi-Buffer ADC (MIBADC)
- External Memory Interface (EMIF) / Parameter Overlay Module (POM)
- NHET (High End Timer) IDE
- NHET
- NHET Transfer Unit
- Summary & Questions



Thank You

Contact Information:
Hoiman Low: hm-low@ti.com



ZHCP003

重要声明

德州仪器(TI) 及其下属子公司有权根据 JESD46 最新标准, 对所提供的产品和服务进行更正、修改、增强、改进或其它更改， 并有权根据 JESD48 最新标准中止提供任何产品和服务。客户在下订单前应获取最新的相关信息, 并验证这些信息是否完整且是最新的。所有产品的销售都遵循在订单确认时所提供的TI 销售条款与条件。

TI 保证其所销售的组件的性能符合产品销售时 TI 半导体产品销售条件与条款的适用规范。仅在 TI 保证的范围内，且 TI 认为 有必要时才会使用测试或其它质量控制技术。除非适用法律做出了硬性规定，否则没有必要对每种组件的所有参数进行测试。

TI 对应用帮助或客户产品设计不承担任何义务。客户应对其使用 TI 组件的产品和应用自行负责。为尽量减小与客户产品和应 用相关的风险，客户应提供充分的设计与操作安全措施。

TI 不对任何 TI 专利权、版权、屏蔽作品权或其它与使用了 TI 组件或服务的组合设备、机器或流程相关的 TI 知识产权中授予 的直接或隐含权限作出任何保证或解释。TI 所发布的与第三方产品或服务有关的信息，不能构成从 TI 获得使用这些产品或服 务的许可、授权、或认可。使用此类信息可能需要获得第三方的专利权或其它知识产权方面的许可，或是 TI 的专利权或其它 知识产权方面的许可。

对于 TI 的产品手册或数据表中 TI 信息的重要部分，仅在没有对内容进行任何篡改且带有相关授权、条件、限制和声明的情况 下才允许进行复制。TI 对此类篡改过的文件不承担任何责任或义务。复制第三方的信息可能需要服从额外的限制条件。

在转售 TI 组件或服务时，如果对该组件或服务参数的陈述与 TI 标明的参数相比存在差异或虚假成分，则会失去相关 TI 组件 或服务的所有明示或暗示授权，且这是不正当的、欺诈性商业行为。TI 对任何此类虚假陈述均不承担任何责任或义务。

客户认可并同意，尽管任何应用相关信息或支持仍可能由 TI 提供，但他们将独力负责满足与其产品及在其应用中使用 TI 产品 相关的所有法律、法规和安全相关要求。客户声明并同意，他们具备制定与实施安全措施所需的全部专业技术和知识，可预见 故障的危险后果、监测故障及其后果、降低有可能造成人身伤害的故障的发生机率并采取适当的补救措施。客户将全额赔偿因 在此类安全关键应用中使用任何 TI 组件而对 TI 及其代理造成的任何损失。

在某些场合中，为了推进安全相关应用有可能对 TI 组件进行特别的促销。TI 的目标是利用此类组件帮助客户设计和创立其特 有的可满足适用的功能安全性标准和要求的终端产品解决方案。尽管如此，此类组件仍然服从这些条款。

TI 组件未获得用于 FDA Class III（或类似的生命攸关医疗设备）的授权许可，除非各方授权官员已经达成了专门管控此类使 用的特别协议。

只有那些 TI 特别注明属于军用等级或“增强型塑料”的 TI 组件才是设计或专门用于军事/航空应用或环境的。购买者认可并同 意，对并非指定面向军事或航空航天用途的 TI 组件进行军事或航空航天方面的应用，其风险由客户单独承担，并且由客户独 力负责满足与此类使用相关的所有法律和法规要求。

TI 已明确指定符合 ISO/TS16949 要求的产品，这些产品主要用于汽车。在任何情况下，因使用非指定产品而无法达到 ISO/TS16949 要求，TI不承担任何责任。

	产品		应用
数字音频	www.ti.com.cn/audio	通信与电信	www.ti.com.cn/telecom
放大器和线性器件	www.ti.com.cn/amplifiers	计算机及周边	www.ti.com.cn/computer
数据转换器	www.ti.com.cn/dataconverters	消费电子	www.ti.com/consumer-apps
DLP® 产品	www.dlp.com	能源	www.ti.com/energy
DSP - 数字信号处理器	www.ti.com.cn/dsp	工业应用	www.ti.com.cn/industrial
时钟和计时器	www.ti.com.cn/clockandtimers	医疗电子	www.ti.com.cn/medical
接口	www.ti.com.cn/interface	安防应用	www.ti.com.cn/security
逻辑	www.ti.com.cn/logic	汽车电子	www.ti.com.cn/automotive
电源管理	www.ti.com.cn/power	视频和影像	www.ti.com.cn/video
微控制器 (MCU)	www.ti.com.cn/microcontrollers		
RFID 系统	www.ti.com.cn/rfidsys		
OMAP应用处理器	www.ti.com/omap		
无线连通性	www.ti.com.cn/wirelessconnectivity	德州仪器在线技术支持社区	www.deyisupport.com

邮寄地址： 上海市浦东新区世纪大道1568 号，中建大厦32 楼邮政编码： 200122